ALGANT MASTER THESIS

S-parts of values of univariate polynomials and decomposable forms

Author
Maurizio MORESCHI

Supervisor
Dr. Jan-Hendrik EVERTSE

Universität Regensburg

Universiteit Leiden

August 2018

S'io avessi le rime aspre e chiocce,
come si converrebbe al tristo buco
sovra 'l qual pontan tutte l'altre rocce,

io premerei di mio concetto il suco
più pienamente; ma perch'io non l'abbo,
non sanza tema a dicer mi conduco;

ché non è impresa da pigliare a gabbo
discriver fondo a tutto l'universo,
né da lingua che chiami mamma o babbo.

Ma quelle donne aiutino il mio verso
ch'aiutaro Anfione a chiuder Tebe,
sì che dal fatto il dir non sia diverso.

(Dante, Inferno C. XXXII, vv. 1-12)

Notation and prerequisites

The main prerequisite in order to be able to understand the work in this thesis is some familiarity with p-adic analysis.

For obvious reasons, this is not the place to give a treatment of such a topic. The reader not familiar with p-adic analysis is invited to have a look at [Kob84].

Some familiarity with algebraic geometry (for example at the level of the first two chapters of [Har77]) would help appreciating more some of the results in chapter 1, but it is not essential for the general understanding of this thesis.

Let $m \in \mathbb{Z}_{\geq 1}$. We denote by μ_∞^m the usual Lebesgue measure on $\mathbb{R}^m$ and by

$$\|\mathbf{x}\| := \max_{i \in \{1,\dots,m\}} |x_i| \qquad (\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{R}^m), \tag{i}$$

the sup-norm of the components in $\mathbb{R}^m$.

Similarly, for any prime number p we denote μ_p^m the Haar measure on $\mathbb{Q}_p^m$ normalized in such a way that $\mu_p^m(\mathbb{Z}_p^m) = 1$. We denote by v_p the p-adic valuation on $\mathbb{Q}_p$ and $|\cdot|_p$ the p-adic absolute value, both with their standard normalizations. Also, we denote

$$\|\mathbf{x}\|_p := \max_{i \in \{1,\dots,m\}} |x_i|_p \qquad (\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{R}^m), \tag{ii}$$

the sup-norm of the components in $\mathbb{Q}_p^m$.

If K_p is a finite extension of $\mathbb{Q}_p$, then the absolute value $|\cdot|_p$ extends uniquely to an absolute value on K_p, with respect to which K_p is complete (cf. [Neu99]). If the extension $K_p/\mathbb{Q}_p$ is fixed in the context, then we may denote the extended absolute value still by $|\cdot|_p$ without any risk of confusion.

Recall that if ϖ is a local uniformizer for K_p, then one has

$$|\varpi|_p = p^{1/e_p}, \tag{iii}$$

where e_p denotes the ramification index of the extension $K_p/\mathbb{Q}_p$.

The ring of adeles of $\mathbb{Q}$ is the subset $\mathbb{A} \subseteq \prod_v \mathbb{Q}_v$ (v running over all places of $\mathbb{Q}$) of all tuples $(x_v)_v$ such $x_v \in \mathbb{Z}_v$ for all but finitely many places v (conventionally $\mathbb{Z}_\infty := \mathbb{R}$). The ring structure and the topology on $\mathbb{A}$ are inherited from the product. We denote by μ^m the restriction to $\mathbb{A}^m$ of the product measure $\bigotimes_v \mu_v^m$.

As a general rule, we always omit the superscript (specifying the dimension) from the notation when $m = 1$. Clearly $\mu_v^m = \mu_v^{\otimes m}$ for any place v of $\mathbb{Q}$ and an easy computation shows that $\mu^m = \mu^{\otimes m}$.

For polynomials $f \in \mathbb{Z}[X_1, \ldots, X_m]$, we also introduce the notation

$$V_f(B, M) := \{\mathbf{x} \in \mathbb{R}^m \,:\, |x| \leq B,\, |f(x)| \leq M\} \qquad (B, M \in \mathbb{R}_{>0}) \tag{iv}$$

and

$$N_h(f) := \#\{\mathbf{x} \in \mathbb{Z}^m / h\mathbb{Z}^m \,:\, f(\mathbf{x}) \equiv 0 \mod h\} \qquad (h \in \mathbb{Z}_{>1}). \tag{v}$$

Additional (and more classical) notation used in the thesis is listed below.

- Approximations of $x \in \mathbb{R}$ by integers:
  - $\lfloor x \rfloor$:= largest integer $\leq x$ (floor of x),
  - $\lceil x \rceil$:= smallest integer $\geq x$ (ceiling of x),
  - $\{x\} := x - \lfloor x \rfloor$ (mantissa of x).
- Vinodograv symbols:
  - $f \ll g$ (for $f \in O(g)$),

- $f \gg g$ (for $g \in O(f)$),
- $f \asymp g$ (for $f \in O(g) \ \wedge \ g \in O(f)$).

When a subscript is present, it specifies the parameters the implied constants depend on.

- Localization of $\mathbb{Z}$ at a prime p:

  $$\mathbb{Z}_{(p)} := \{x/p^k \ : \ x \in \mathbb{Z}, \, k \in \mathbb{Z}_{\geq 0}\} \subseteq \mathbb{Q}.$$

- Subspaces of a vector space:

  If V is a vector space over a field K, then the notation $W \leq V$ means that W is a K-vector subspace of V.

- Algebraic geometry:
  - We use the notation Spec and Proj to refer to the corresponding usual costructions in algebraic geometry (see [Har77]).
  - By the term *variety*, we always mean a separated integral scheme of finite type over a field.

Contents

Chapter 0

Introduction

Let S be a finite non-empty set of primes. For any $y \in \mathbb{Z}_{\neq 0}$, let

$$|y| = \prod_p p^{v_p(y)} \tag{1}$$

be the prime factorization of $|y|$, where p runs over the set of all prime numbers. The *S-part* of y is defined by

$$[y]_S := \prod_{p \in S} p^{v_p(y)}. \tag{2}$$

In the present work, we are interested in comparing the S-parts of (non-zero) values of univariate polynomials and decomposable forms with small powers of their absolute values.

For univariate polynomials, the first general result in this direction was established by Gross and Vincent in [GV13] as a generalization of a result of Stewart ([Ste84]).

Theorem ([GV13])**.** *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial with at least two distinct roots and let S be a finite, non-empty set of primes. Then there exist effectively computable constants $\kappa_1, \kappa_2 > 0$, depending only on f and S, such that, for any $x \in \mathbb{Z}$ with $f(x) \neq 0$, one has*

$$[f(x)]_S < \kappa_2 |f(x)|^{1-\kappa_1}.$$

In [BEG18], Bugeaud, Evertse and Győry proved the following ineffective version of the result of Gross and Vincent for polynomials of non-zero discriminant.

Theorem ([BEG18, Theorem 2.1]). *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ and non-zero discriminant, and let S be a non-empty finite set of primes. Then, for any $\delta > 0$ and any $x \in \mathbb{Z}$ with $f(x) \neq 0$, one has*

$$[f(x)]_S \ll_{f,S,\delta} |f(x)|^{(1/n)+\delta}.$$

Furthermore, the exponent $1/n$ is the best possible, in the sense that there exist infinitely many primes p and infinitely many $x \in \mathbb{Z}$ such that $f(x) \neq 0$ and

$$[f(x)]_{\{p\}} \gg_{f,p} |f(x)|^{1/n}.$$

If $\varepsilon \in \left(0, \frac{1}{n}\right)$, then the set of integers x such that $0 < |f(x)|^\varepsilon \leq [f(x)]_S$ may be infinite (in fact it is every time f has a root in $\mathbb{Z}_p$ for some $p \in S$). However, as one may expect, such a set has natural density zero, i.e.

$$\lim_{B\to\infty} \frac{\#\{x \in \mathbb{Z} : |x| \leq B, 0 < |f(x)|^\varepsilon \leq [f(x)]_S\}}{B} = 0. \tag{3}$$

A natural question that arises concerns the exact growth rate of the quantity

$$N(f, S, \varepsilon, B) := \#\{x \in \mathbb{Z} : |x| \leq B, 0 < |f(x)|^\varepsilon \leq [f(x)]_S\} \tag{4}$$

as $B \to \infty$.

Bugeaud, Evertse and Gyõry considered this problem and proved the following result.

Theorem ([BEG18, Theorem 2.3]). *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ and non-zero discriminant $\Delta \neq 0$. Let S be a finite set of primes and let $S' \subseteq S$ be the subset of all $p \in S$ such that f has a root in $\mathbb{Z}_p$. Suppose that $s' := \#S' \geq 1$. Then, for any $\varepsilon \in \left(0, \frac{1}{n}\right)$, one has*

$$N(f, S, \varepsilon, B) \asymp_{f,S,\varepsilon} B^{1-n\varepsilon}(\log B)^{s'-1} \quad \text{as } B \to \infty.$$

A preliminary version of [BEG18] dating back to August 2017 contained the remark that the limit

$$\lim_{B\to\infty} \frac{N(f, S, \varepsilon, B)}{B^{1-n\varepsilon}(\log B)^{s'-1}} \tag{5}$$

may not exist.

The reason behind such remark was, in our opinion, that in the case $s' = 1$ it is easy to construct sequences $(B_l)_l$, $(B'_l)_l$ along which the limits

$$\lim_{l\to\infty} \frac{N(f,S,\varepsilon,B_l)}{B_l^{1-n\varepsilon}}, \quad \lim_{l\to\infty} \frac{N(f,S,\varepsilon,B'_l)}{B_l'^{1-n\varepsilon}} \tag{6}$$

exist but differ from each other.

However, the construction of such sequences deeply relies on the fact that if $S' = \{p\}$, then the quotient of two consecutive elements of the set $\{p^k : k \in \mathbb{Z}_{\geq 0}\}$ in the increasing order is constant, so it does not generalize to general s'. This is due to the fact that if $S' = \{p_1, \ldots, p_{s'}\}$, with $s' \geq 2$, and $(h_l)_l$ is the sequence of the elements of the set

$$\mathbb{N}_{S'} := \{p_1^{k_1} \ldots p_{s'}^{k_{s'}} : (k_1, \ldots, k_{s'}) \in \mathbb{Z}_{\geq 0}^{s'}\} \tag{7}$$

in increasing order, then equidistribution theory tells us that $h_{l+1}/h_l \to 1^+$ as $l \to \infty$.

This led us to the idea of using equidistribution theory to study the limit (5) in the case $s' \geq 2$. Thanks to a result of Everest ([Eve92, Theorem 1]) in this field, we managed to refined the result of Bugeaud, Evertse and Győry to an exact asymptotic.

Theorem I. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ and non-zero discriminant, and let $\varepsilon \in \left(0, \frac{1}{n}\right)$. Also, let S be a finite set of primes and let $S' \subseteq S$ be the subset of all $p \in S$ such that f has a root in $\mathbb{Z}_p$. Suppose that $s' := \#S' > 1$. Then there exists a constant $C(f,S,\varepsilon) > 0$ such that*

$$N(f,S,\varepsilon,B) \sim C(f,S,\varepsilon) \cdot B^{1-n\varepsilon} (\log B)^{s'-1} \quad \textit{as } B \to \infty.$$

An explicit formula for $C(f,S,\varepsilon)$ is given in chapter 3, from which the precise dependence on f, S and ε can be clearly read off.

In fact, Everest's result does not need the elements of S' to be prime numbers, but only that the set S' is $\mathbb{Q}$-multiplicatively independent (i.e. that the set $\{\log p_1, \dots, \log p_{s'}\}$ is $\mathbb{Q}$-linearly independent). We can thus consider, more generally, $\mathbb{Q}$-multiplicatively independent subsets $\Sigma = \{q_1, \dots, q_s\}$ of $\mathbb{R}_{>1}$, with $s \geq 2$. We denote

$$\mathbb{N}_\Sigma := \{q_1^{k_1} \dots q_s^{k_s} \,:\, (k_1, \dots, k_s) \in \mathbb{Z}_{\geq 0}^s\} \tag{8}$$

For each $h \in \mathbb{N}_\Sigma$ the numbers $v_{q_1}(h), \dots, v_{q_s}(h) \in \mathbb{Z}_{\geq 0}$ are uniquely determined by the writing

$$h = q_1^{v_{q_1}(h)} \dots q_s^{v_{q_s}(h)}. \tag{9}$$

Let $\alpha, \alpha' \in \mathbb{R}_{>0}$, $\nu_1, \dots \nu_s \in \mathbb{Z}_{\geq 1}$ and $L \in \mathbb{R}_{>1}$. Combining Everest's result with some elementary analytic considerations, we determine in chapter 2 the asymptotic rate as $L \to \infty$ of sums of the form

$$\sum_{h \in \mathbb{N}_\Sigma} v_{q_1}(h)^{\nu_1 - 1} \dots v_{q_s}(h)^{\nu_s - 1} \min\{h^\alpha, L^{\alpha+\alpha'} h^{-\alpha'}\}. \tag{10}$$

Besides yielding results which are interesting on their own right, the results from chapter 2 lead to fruitful applications to the study of S-parts of values of polynomials with zero discriminant and decomposable forms. The bridge is given by the theory of Igusa local zeta functions, which constitute the topic of chapter 1 of this thesis.

For general univariate polynomials we prove the following result in chapter 3.

Theorem II. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 1$, let S be a finite set of primes and let $S' \subseteq S$ be the subset of all $p \in S$ such that f has a root in $\mathbb{Z}_p$. Suppose that $s' := \#S' \geq 1$ and denote by $R(f)$ the maximum multiplicity of a root of f in an algebraic closure of $\mathbb{Q}$. Then for any $\varepsilon \in \left(0, \frac{1}{n}\right)$ one has*

$$N(f, S, \varepsilon, B) \asymp_{f,S,\varepsilon} B^{1-(n\varepsilon)/R(f)} (\log B)^{s'-1} \quad \text{as } B \to \infty.$$

In the case of decomposable forms $F \in \mathbb{Z}[X_1, \dots, X_m]$ $(m \geq 2)$, that is homogeneous polynomials that can be written as product of linear forms over algebraic closure of $\mathbb{Q}$, given the homogeneity constraint, we restrict to values at primitive points in $\mathbb{Z}^m$, i.e. $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m$ with $\gcd(x_1, \dots, x_m) = 1$. We denote $\mathbb{Z}^m_{\text{prim}}$ the subset of all primitive points of $\mathbb{Z}^m$ and for any $\varepsilon, B, \gamma \in \mathbb{R}_{>0}$ we define

$$N(F, S, \varepsilon, B) := \#\{\mathbf{x} \in \mathbb{Z}^m_{\text{prim}} \ : \ \|\mathbf{x}\| \leq B,\, 0 < |F(\mathbf{x})|^{\varepsilon} \leq [F(\mathbf{x})]_S\}. \qquad (11)$$

Clearly all binary forms $F \in \mathbb{Z}[X, Y]$ are decomposable. For binary forms of non-zero discriminant Bugeaud, Evertse and Győry proved the following result.

Theorem ([BEG18]). *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a binary form of degree $n > 2$ and non-zero discriminant. Also, let S be a finite set of primes and let $S' \subseteq S$ be the subset of all $p \in S$ such that F has a non-trivial zero in $\mathbb{Z}_p^2$. Suppose that $s' := \#S' > 0$. Then, for any $\varepsilon \in \left(0, \frac{1}{n}\right)$, one has*

$$N(F, S, \varepsilon, B) \asymp_{F,S,\varepsilon} B^{1-n\varepsilon}(\log B)^{s'-1} \quad \text{as } B \to \infty.$$

A notion of discriminant for general decomposable forms has been introduced by Evertse and Győry in [EG92]. In chapter 4, we generalize the above result to any decomposable form of non-zero discriminant.

Theorem III. *Let $F \in \mathbb{Z}[X_1, \dots, X_m]$ $(m \geq 2)$ be a decomposable form of degree $n > m$ and non-zero discriminant. Also, let S be a finite set of primes and let $S' \subseteq S$ be the subset of all $p \in S$ such that F has a non-trivial zero in $\mathbb{Z}_p^m$. Suppose $s' := \#S' \geq 1$. Then, for any $\varepsilon \in \left(0, \frac{1}{n}\right)$, one has*

$$N(F, S, \varepsilon, B) \asymp_{F,S,\varepsilon} B^{m-n\varepsilon}(\log B)^{\nu-1} \quad \text{as } B \to \infty$$

for some

$$\nu \in \mathbb{Z} \cap [s', (m-1)s']$$

More generally, for a decomposable form $F = L_1^{r_1} \dots L_l^{r_l} \in \mathbb{Z}[X_1, \dots, X_m]$, with $L_1, \dots, L_l \in \mathbb{C}[X_1, \dots, X_m]$ linear forms with distinct support, we denote

$$\operatorname{rk}(F) := \operatorname{rk}(L_1, \dots, L_l), \qquad (12)$$

$$\mathcal{L}(F) := \left\{ W \le \mathbb{C}^n \,:\, \exists I \subseteq \{1,\dots,r\}, W = \bigcap_{i\in I}\{L_i = 0\} \right\} \tag{13}$$

and

$$q(F) := \max_{\substack{W\in\mathcal{L}(F)\\ 1\le \operatorname{codim} W \le \min\{\operatorname{rk}(F), m-1\}}} \frac{\sum_{L_i\supseteq W} r_i}{\operatorname{codim} W}. \tag{14}$$

We say that a form $F \in \mathbb{Z}[X_1,\dots,X_m]$ is *of finite type* if

$$\operatorname{vol}(F) := \mu_\infty^m\{\mathbf{x}\in\mathbb{R}^m \,:\, |F(\mathbf{x})| \le 1\} < \infty. \tag{15}$$

For decomposable forms of finite type, we prove in chapter 4 the following result.

Theorem IV. *Let $F \in \mathbb{Z}[X_1,\dots,X_m]$ $(m \ge 2)$ be a decomposable form of degree $n > m$ and of finite type. Also, let S be a finite set of primes and let $S' \subseteq S$ be the subset of all $p \in S$ such that F has a non-trivial zero in $\mathbb{Z}_p^m$. Suppose $s' := \#S' \ge 1$. Then, for any $\varepsilon \in \left(0, \frac{1}{n}\right)$, one has*

$$N(F,S,\varepsilon,B) \asymp_{F,S,\varepsilon} B^{m-(n\varepsilon)/q(F)}(\log B)^{\nu-1} \quad \text{as } B\to\infty$$

for some

$$\nu \in \mathbb{Z}\cap[s', (m-1)s'].$$

Chapter 1

Igusa local zeta functions

Let $f(X_1, \ldots, X_m) \in \mathbb{Z}_p[X_1, \ldots, X_m]$. The *Igusa zeta function of f (at p)* is the holomorphic function on the right half-plane defined by

$$\zeta_{f,p}(s) := \int_{\mathbb{Z}_p^m} |f(x)|_p^s \, d\mu_p^m(x) \quad (s \in \mathbb{C} : \Re(s) > 0). \tag{1.1}$$

We may write

$$\zeta_{f,p}(s) = Z_{f,p}(p^{-s}), \tag{1.2}$$

where

$$Z_{f,p}(T) := \sum_{k=0}^{\infty} \mu_p^m(\{\mathbf{x} \in \mathbb{Z}_p^m : |f(\mathbf{x})|_p = p^{-k}\})\, T^k \in \mathbb{Z}_{(p)}[\![T]\!]. \tag{1.3}$$

In [Igu74], Igusa proved that $Z_{f,p}(T)$ is a rational function of T, which implies that $\zeta_{f,p}(s)$ has a meromorphic extension to $\mathbb{C}$. In fact, Igusa's result gives also a list of candidates for the poles of the Dirichlet $Z_{f,p}(p^{-s})$ in terms of numerical data of log-resolutions of singularities of the pair

$$\Big(\operatorname{Spec}\big(\mathbb{Q}_p[X_1, \ldots, X_m]\big), \operatorname{Spec}\big(\mathbb{Q}_p[X_1, \ldots, X_m]/(f)\big)\Big). \tag{1.4}$$

In section 1.1 we explain the relation between the Igusa local zeta functions and log resolution of singularities. We also introduce and study the notion of log-canonical threshold, which is of central importance in this thesis.

In section 1.2 we state Igusa's theorem and the consequent asymptotic bounds on the power series coefficients of (1.3).

In section 1.3 we introduce slight variations on Igusa local zeta functions in the homogeneous context and we prove an important result on decomposable forms.

1.1 Log-resolutions and log-canonical thresholds

Definition 1.1.1. *Let X be a smooth variety of dimension m over a field K. A Weil divisor $D = \sum_{i\in I} D_i$ on X is a simple normal crossing divisor if*

1. *D_i is smooth, irreducible and of codimension one for all $i \in I$, and*
2. *for any $P \in Supp(D)$ there exists independent local parameters $x_1, \ldots, x_r \in \mathcal{O}_{X,P}$ such that D is given, around P, by the local equation*

$$x_1 \ldots x_r = 0.$$

Definition 1.1.2. *Let X be a smooth variety over a field K and let D be a Weil divisor on X. A log-resolution of the pair (X, D) is a proper birational morphism $h : Y \to X$ such that Y is smooth and $h^*D = \sum_{i\in I} N_i E_i$ $(N_i \in \mathbb{Z}_{\geq 1}\ \forall i \in I)$ for some simple normal crossing divisor E with irreducible components $(E_i)_{i\in I}$ on Y.*

A priori there is no reason why a log-resolutions would exist. Over fields of characteristic zero their existence is a celebrated result of Hironaka.

Theorem 1.1.3 (Hironaka)**.** *Let X be a smooth variety over a field of characteristic zero. Then for any Weil divisor D on X the pair (X, D) admits a log-resolution.*

Let X be a smooth variety over a field K of characteristic zero, let D be a Weil divisor on X and let $h : Y \to X$ be a log-resolution of the pair (X, D), with $h^*D = \sum_{i\in I} N_i E_i$ for a simple normal crossing divisor E with irreducible components $(E_i)_{i\in I}$ on Y. One can show that the relative canonical divisor $\mathcal{K}_Y - h^*\mathcal{K}_X$ is numerically equivalent to a divisor $\sum_{i\in I}(k_i - 1)E_i$ for some $k_i \in \mathbb{Z}_{\geq 1}$ $(i \in I)$. The (finite) set of pairs $\{(N_i, k_i)\}_{i\in I}$ is called the *numerical data* of the log-resolution h.

A fundamental property of log-resolutions is that the quantity

$$\operatorname{lct}(X, D) := \min_{i \in I} \frac{k_i}{N_i} \tag{1.5}$$

is independent of the choice of the resolution h (see [Laz04]).

The quantity (1.5) is called the log-canonical threshold of the pair (X, D). We also introduce the following notation.

Definition 1.1.4. *Let K be a field of characteristic zero and let $f \in K[X_1, \ldots, X_m]$. We define the log-canonical threshold of f over K by*

$$\operatorname{lct}_K(f) := \operatorname{lct}\Big(\operatorname{Spec}\left(K[X_1, \ldots, X_m]\right), \operatorname{Spec}\left(K[X_1, \ldots, X_m]/(f)\right)\Big).$$

The following result on log-canonical thresholds is very important for our purposes. Not having found an adequate reference for it, we also include a proof.

Theorem 1.1.5. *Let $f \in \mathbb{Z}[X_1, \ldots, X_m]$ and let K be any field of characteristic zero. Then $\mathbb{Q}$ embeds in K and one has*

$$\operatorname{lct}_{\mathbb{Q}}(f) \geq \operatorname{lct}_K(f).$$

Moreover, if f is univariate or homogeneous, then the equality holds.

Proof. Since the characteristic of K is zero, one has $b \cdot 1_K \neq 0$ for all $b \in \mathbb{Z}_{>0}$. Therefore we get a well-defined embedding $\mathbb{Q} \hookrightarrow K$ by sending a/b to $(a \cdot 1_K) \cdot (b \cdot 1_K)^{-1}$ for all $a \in \mathbb{Z}, b \in \mathbb{Z}_{>0}$. Let $\iota : \mathbb{Q}[X_1, \ldots, X_m] \hookrightarrow K[X_1, \ldots, X_m]$ denote the induced inclusion.

Consider a log-resolution

$$h : Y \to \operatorname{Spec}(\mathbb{Q}[X_1, \ldots, X_m])$$

of the pair $\big(\operatorname{Spec}(\mathbb{Q}[X_1, \ldots, X_m]), \operatorname{Spec}(\mathbb{Q}[X_1, \ldots, X_m]/(f))\big)$.

We have the cartesian square

$$\begin{array}{ccc} Y_K & \xrightarrow{h_K} & \mathrm{Spec}(K[X_1,\ldots,X_m]) \\ \pi \downarrow & & \downarrow \mathrm{Spec}(\iota) \\ Y & \xrightarrow[h]{} & \mathrm{Spec}(\mathbb{Q}[X_1,\ldots,X_m]), \end{array}$$

where $Y_K := Y \times_{\mathrm{Spec}(\mathbb{Q}[X_1,\ldots,X_m])} \mathrm{Spec}(K[X_1,\ldots,X_m])$. It is easy to check that the birational map

$$h_K : Y_K \to \mathrm{Spec}(K[X_1,\ldots,X_m])$$

is a log-resolution of the pair $\big(\mathrm{Spec}(K[X_1,\ldots,X_m]), \mathrm{Spec}(K[X_1,\ldots,X_m]/(f))\big)$.

Now, suppose that $h^* \mathrm{Spec}(\mathbb{Q}[X_1,\ldots,X_m]/(f)) = \sum_{i\in I} N_i E_i$ for a simple normal crossing divisor E with irreducible components $(E_i)_{i\in I}$ on Y. The E_i's might not be irreducible anymore after base change, let say they decompose as

$$E_i \times_{\mathrm{Spec}(\mathbb{Q}[X_1,\ldots,X_m])} \mathrm{Spec}(K[X_1,\ldots,X_m]) = \sum_{j\in J_i} a_j E'_j,$$

with $a_j \in \mathbb{Z}_{>0}$ and E'_j irreducible for all $j \in J_i$.

Therefore, if h had numerical data $\{(N_i,k_i)\}_{i\in I}$, the numerical data of h_K are given by $\{(N'_j,k'_j)\}_{j\in J}$, where

$$J = \bigcup_{i\in I} J_i$$

and

$$(N'_j,k'_j) = (a_j N_i, a_j(k_i-1)+1) \quad \text{if } j \in J_i.$$

It follows that

$$\mathrm{lct}_K(f) = \min_{j\in J} \frac{a_j(k_i-1)+1}{a_j N_i} = \min_{i\in I}\left(\frac{k_i}{N_i} - \frac{1}{N_i}\max_{j\in J_i}\left(1-\frac{1}{a_j}\right)\right) \leq \mathrm{lct}_{\mathbb{Q}}(f). \quad (1.6)$$

It is also clear that the equality in (1.6) holds if and only if $a_j = 1$ for all $j \in J$. We claim that this is always the case if f is univariate or homogenous.

If f is univariate, then we may consider its irreducible factorization

$$f = c\, g_1^{r_1} \dots g_l^{r_l}$$

in $\mathbb{Z}[X]$, where the g_i's are irreducible primitive pairwise coprime polynomials with integer coefficients, $c \in \mathbb{Z}_{\neq 0}$ and $r_i \in \mathbb{Z}_{>0}$ for all $i \in \{1, \dots, l\}$. Then we see that $I = \{1, \dots, l\}$ and, for all $i \in I$, E_i is the proper transform of $\operatorname{Spec}(\mathbb{Q}[X_1, \dots, X_m]/(g_i))$. Since all $g_i \in \mathbb{Z}[X]$ are irreducible over $\mathbb{Q}$ (and $\mathbb{Q}$ has characteristic zero), they are also separable. In particular, they cannot have multiple factors in $K[X]$, from which the claim follows.

If f is homogeneous, then a log-resolution

$$h : Y \to \operatorname{Spec}(\mathbb{Q}[X_1, \dots, X_m])$$

of the pair $\big(\operatorname{Spec}(\mathbb{Q}[X_1, \dots, X_m]), \operatorname{Spec}(\mathbb{Q}[X_1, \dots, X_m]/(f))\big)$ can be obtained as a composition of birational maps

$$Y \xrightarrow{h_0} \operatorname{Proj}(\mathbb{Q}[X_1, \dots, X_m]) \xrightarrow{pr} \operatorname{Spec}(\mathbb{Q}[X_1, \dots, X_m]),$$

where

$$h_0 : Y \to \operatorname{Proj}(\mathbb{Q}[X_1, \dots, X_m])$$

is a log-resolution of the pair $\big(\operatorname{Proj}(\mathbb{Q}[X_1, \dots, X_m]), \operatorname{Proj}(\mathbb{Q}[X_1, \dots, X_m]/(F))\big)$ and

$$\operatorname{Proj}(\mathbb{Q}[X_1, \dots, X_m]) \xrightarrow{pr} \operatorname{Spec}(\mathbb{Q}[X_1, \dots, X_m])$$

is the "projection" map from the Proj construction.

The exceptional divisors of h are given by the proper transform (under h_0) of the exceptional divisor of pr and by the exceptional divisors of h_0. The former stays irreducible under the base change induced by the field extension $\mathbb{Q} \hookrightarrow K$ and gives a numerical datum (n, m). On the other hand, the exceptional divisors of h_0 are projective, so, if

$$h_0^* \operatorname{Proj}(\mathbb{Q}[X_1, \dots, X_m]/(f)) = \sum_{i \in I_0} N_i E_i$$

for a simple normal crossing divisor E^0 with irreducible components $(E_i)_{i\in I_0}$ on Y, then the E_i's are smooth, projective and of codimension one by definition of simple normal crossing divisor. These properties still hold after the base change, with the consequence that the divisors

$$E_i \times_{\mathrm{Proj}(\mathbb{Q}[X_1,\ldots,X_m])} \mathrm{Proj}(K[X_1,\ldots,X_m]) \quad (i \in I_0)$$

cannot have multiple irreducible components. □

The proof of theorem 1.1.5 incidentally computes the log-canonical thresholds of univariate polynomials.

Corollary 1.1.6. *Let $f \in \mathbb{Z}[X]$ be a univariate polynomial of degree $n \geq 1$ and denote $R(f)$ the maximum multiplicity of a root of f in an algebraic closure of $\mathbb{Q}$. Then for any field K of characteristic zero one has*

$$\mathrm{lct}_K(f) = \frac{1}{R(f)}.$$

Proof. Clear. □

In a homogeneous context, we may give the following "projective" analogue of definition 1.1.4.

Definition 1.1.7. *Let K be a field of characteristic zero and let $F \in K[X_1,\ldots,X_m]$ be a form. We define the* projective log-canonical threshold *of F over K by*

$$\mathrm{plct}_K(F) := \mathrm{lct}_K\Big(\mathrm{Proj}\,(K[X_1,\ldots,X_m]), \mathrm{Proj}\,(K[X_1,\ldots,X_m]/(F))\Big).$$

Corollary 1.1.8. *Let $F \in \mathbb{Z}[X_1,\ldots,X_m]$ be a form and let K be any field of characteristic zero. Then*

$$\mathrm{plct}_{\mathbb{Q}}(F) = \mathrm{plct}_K(F).$$

Proof. It follows immediately from the proof of theorem 1.1.5. □

1.2 Igusa's theorem and its consequences

Before stating Igusa's theorem, let us prove the following result characterizing the cases in which $Z_{f,p}(T)$ is a polynomial.

Lemma 1.2.1. *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$. Then $Z_{f,p}(T) \in \mathbb{Z}_{(p)}[T]$ if and only if f has a zero in $\mathbb{Z}_p^m$.*

Proof. Note first that, since the polynomial function $f : \mathbb{Z}_p^m \to \mathbb{Z}_p$ is continous, so is also the composition $|f|_p : \mathbb{Z}_p^m \to p^{\mathbb{Z}_{\leq 0}} \cup \{0\}$. Consequently, the image of $|f|_p$ is compact.

Now, if f has no zeros in $\mathbb{Z}_p^m$, then the image of $|f|_p$ is contained in the discrete subset $p^{\mathbb{Z}_{\leq 0}}$, so it is finite. This implies that $Z_{f,p}(T) \in \mathbb{Z}_{(p)}[T]$.

On the contrary, if f has a zero in $\mathbb{Z}_p^m$, then 0 is an accumulation point for the image of $|f|_p$. Therefore, there exist infinitely many $k \in \mathbb{Z}_{\geq 0}$ such that the set

$$\{\mathbf{x} \in \mathbb{Z}_p^m \ : \ |f(\mathbf{x})|_p = p^{-k}\} \tag{1.7}$$

is non-empty. Since the set (1.7) is also open, it follows that it has positive measure and thus $Z_{f,p}(T) \notin \mathbb{Z}_{(p)}[T]$. □

We are now ready to state Igusa's theorem.

Theorem 1.2.2 ([Igu74]). *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ be a polynomial with a zero in $\mathbb{Z}_p^m$. Also, let*

$$h : Y \to \mathrm{Spec}(\mathbb{Q}_p[X_1, \ldots, X_m])$$

be a log-resolution of the pair $\left(\mathrm{Spec}(\mathbb{Q}_p[X_1, \ldots, X_m]), \mathrm{Spec}(\mathbb{Q}_p[X_1, \ldots, X_m]/(f))\right)$ with numerical data $\{(N_i, k_i)\}_{i \in I}$. Then there exists a polynomial $A \in \mathbb{Z}_{(p)}[T]$ such that

$$Z_{f,p}(T) = \frac{A(T)}{\prod_{i \in I}(1 - p^{-k_i} T^{N_i})}.$$

Moreover, the order of a pole $s = s_0 \in \mathbb{C}$ of $Z_{f,p}(p^{-s})$ is less or equal than

$$\max\left\{\#J \ : \ J \subseteq I, \ -\frac{k_j}{N_j} = \Re(s_0) \, \forall j \in J, \ \bigcap_{j \in J} E_j(\mathbb{Q}_p) \neq \bigcup_{J \subsetneq J' \subseteq I} \bigcap_{j' \in J'} E_{j'}(\mathbb{Q}_p)\right\}.$$

Remark 1.2.3. *Using the properties of normal crossing divisors (cf.* [Laz04, chapter 4]*), it is not difficult to show that*

$$\max\left\{\#J\ :\ J\subseteq I,\ -\frac{k_j}{N_j}=\Re(s_0)\,\forall j\in J,\ \bigcap_{j\in J}E_j(\mathbb{Q}_p)\neq\bigcup_{J\subsetneq J'\subseteq I}\ \bigcap_{j'\in J'}E_{j'}(\mathbb{Q}_p)\right\}\leq m.$$

We introduce now the two quantities related to the Dirichlet series $Z_{f,p}(p^{-s})$ which are of most interest to us, namely $\sigma_p(f)$ and $\nu_p(f)$.

Definition 1.2.4. *Let $f(X_1,\ldots,X_m)\in\mathbb{Z}_p[X_1,\ldots,X_m]$ be a polynomial with a zero in $\mathbb{Z}_p^m$. We denote by $\sigma_p(f)$ the abscissa of convergence of the Dirichlet series $Z_{f,p}(p^{-s})$.*

From theorem 1.2.2, we see that the real part of any of the poles of the Dirichlet series $Z_{f,p}(p^{-s})$ is a negative rational number and $\sigma_p(f)$ equals the maximum of the real parts of such poles.

Note also that the log-canonical threshold $\mathrm{lct}_{\mathbb{Q}_p}(f)$ appears in the set

$$\left\{\frac{k_i}{N_i}\ :\ i\in I\right\} \tag{1.8}$$

corresponding to any possible choice of the log-resolution h in theorem 1.2.2. It is therefore natural to expect that $\sigma_p(f)=-\mathrm{lct}_{\mathbb{Q}_p}(f)$. It is not difficult to show that this is the case indeed.

Proposition 1.2.5. *Let $f(X_1,\ldots,X_m)\in\mathbb{Z}_p[X_1,\ldots,X_m]$ be a polynomial with a zero in $\mathbb{Z}_p^m$. Then*

$$\sigma_p(f)=-\mathrm{lct}_{\mathbb{Q}_p}(f).$$

Proof. Let $\mathbf{a}\in\mathbb{Z}_p^m$ be a zero of f and consider the polynomial

$$g(\mathbf{X}):=f(\mathbf{X}+\mathbf{a})\in\mathbb{Z}_p[\mathbf{X}],$$

where we denote $\mathbf{X}:=(X_1,\ldots,X_m)$. It is easy to check that $\sigma_p(f)=\sigma_p(g)$ and $\mathrm{lct}_{\mathbb{Q}_p}(f)=\mathrm{lct}_{\mathbb{Q}_p}(g)$. Then the result follows from [VZG08, Theorem 2.7]. □

Another fact that is clear from theorem 1.2.2 is that poles of the Dirichlet series $Z_{f,p}(p^{-s})$ with the same real part are of the same order, which makes the following definition meaningful.

Definition 1.2.6. *We denote by $\nu_p(f)$ the order of any pole of $Z_{f,p}(p^{-s})$ on the line $\Re(s) = \sigma_p(f)$.*

Using standard techniques from analytic combinatorics ([FS09, Theorem IV9]) one can deduce from theorem 1.2.2 an asymptotics on the power series coefficients of (1.3). See [Seg11] for the detailed computation.

Corollary 1.2.7. *Let $f(X_1, \ldots, X_m) \in \mathbb{Z}_p[X_1, \ldots, X_m]$ be a polynomial with a zero in $\mathbb{Z}_p^m$. Then*

$$\mu_p^m(\{\mathbf{x} \in \mathbb{Z}_p^m : |f(\mathbf{x})|_p = p^{-k}\}) \ll_{f,p} k^{\nu_p(f)-1} p^{\sigma_p(f)\cdot k} \quad \text{as } k \to \infty$$

and

$$\mu_p^m(\{\mathbf{x} \in \mathbb{Z}_p^m : |f(\mathbf{x})|_p = p^{-k_l}\}) \gg_{f,p} k_l^{\nu_p(f)-1} p^{\sigma_p(f)\cdot k_l} \quad \text{as } l \to \infty$$

for some arithmetic progression $(k_l)_l$.

1.3 Primitive Igusa local zeta functions

In a homogeneous setting, we introduce the following slight variations on Igusa local zeta functions. Let $F(X_1, \ldots, X_m) \in \mathbb{Z}_p[X_1, \ldots, X_m]$ be a form (i.e. a homogeneous polynomial). We define the *primitive Igusa zeta function of F (at p)* to be the holomorphic function on the right half-plane defined by

$$\zeta_{F,p}^*(s) := \int_{\{\mathbf{x} \in \mathbb{Z}_p^m : \|\mathbf{x}\|_p = 1\}} |F(\mathbf{x})|_p^s \, d\mu_p^m(\mathbf{x}), \tag{1.9}$$

with associated power series

$$Z_{F,p}^*(T) := \sum_{k=0}^{\infty} \mu_p^m(\{\mathbf{x} \in \mathbb{Z}_p^m : \|\mathbf{x}\|_p = 1, |F(\mathbf{x})|_p = p^{-k}\}) \, T^k \in \mathbb{Z}_{(p)}[\![T]\!]. \tag{1.10}$$

Note that

$$\begin{aligned} Z_{F,p}(T) &= Z^*_{F,p}(T) + \sum_{k=0}^{\infty} \mu_p^m(\{\mathbf{x} \in p\,\mathbb{Z}_p^m \,:\, |F(\mathbf{x})|_p = p^{-k}\})\, T^k \\ &= Z^*_{F,p}(T) + p^{-m}T^n \cdot Z_{F,p}(T) \end{aligned} \tag{1.11}$$

and thus

$$Z^*_{F,p}(T) = (1 - p^{-m}T^n)\, Z_{F,p}(T). \tag{1.12}$$

We deduce from (1.12) that the power series $Z^*_{F,p}(T)$ is of the same form as in theorem 1.2.2 and thus the whole discussion in section 1.2 has an immediate analogue for $Z^*_{F,p}(T)$.

By an argument similar to the one in [VZG08], one can prove that $Z^*_{F,p}(T) \in \mathbb{Z}_{(p)}[T]$ if and only if F has no non-trivial zeros in $\mathbb{Z}_p^m$.

Definition 1.3.1. *Let $F(X_1, \ldots, X_m) \in \mathbb{Z}_p[X_1, \ldots, X_m]$ be a form with a non-trivial zero in $\mathbb{Z}_p^m$. We denote by $\sigma_p^*(F)$ the abscissa of convergence of the Dirichlet series $Z^*_{F,p}(p^{-s})$ and by $\nu_p^*(F)$ the order of any pole of $Z^*_{F,p}(p^{-s})$ on the line $\Re(s) = \sigma_p^*(F)$.*

From (1.12), we see that

- if $\sigma_p(F) \neq -\frac{m}{n}$, then $\sigma_p^*(F) = \sigma_p(F)$ and $\nu_p^*(F) = \nu_p(F)$;
- if $\sigma_p(F) = -\frac{m}{n}$ and $\nu_p(F) \geq 2$, then $\sigma_p^*(F) = \sigma_p(F)$ and $\nu_p^*(F) = \nu_p(F) - 1$;
- if $\sigma_p(F) = -\frac{m}{n}$ and $\nu_p(F) = 1$, then, because of the assumption $Z^*_{F,p}(T) \notin \mathbb{Z}_{(p)}[T]$, the Dirichlet series $Z_{F,p}(p^{-s})$ has a pole of real part different from $-\frac{m}{n}$. In this case, one has
$$\sigma_p^*(F) = \max\left\{\Re(\xi) \,:\, \xi \text{ is a pole of } Z_{F,p}(p^{-s}) \text{ and } \Re(\xi) \neq -\frac{m}{n}\right\}$$
and $\nu_p^*(F)$ is the order of any pole of $Z_{F,p}(p^{-s})$ on the line $\Re(s) = \sigma_p^*(F)$.

In the homogeneous setting, Igusa's theorem can be improved as follows.

Theorem 1.3.2. *Let $F \in \mathbb{Z}_p[X_1, \ldots, X_m]$ be a form with a non-trivial zero in $\mathbb{Z}_p^m$. Also, let*

$$h_0 : Y \to \mathrm{Proj}(\mathbb{Q}_p[X_1, \ldots, X_m])$$

be a log-resolution of the pair $\big(\mathrm{Proj}(\mathbb{Q}_p[X_1, \ldots, X_m]), \mathrm{Proj}(\mathbb{Q}_p[X_1, \ldots, X_m]/(F))\big)$ with numerical data $\{(N_i, k_i)\}_{i \in I_0}$. Then there exists a polynomial $A \in \mathbb{Z}_{(p)}[T]$ such that

$$Z^*_{F,p}(T) = \frac{A(T)}{\prod_{i \in I_0}(1 - p^{-k_i}T^{N_i})}.$$

Moreover, the order of a pole $s = s_0 \in \mathbb{C}$ of $Z^*_{F,p}(p^{-s})$ is less or equal than

$$\max\Big\{\#J \,:\, J \subseteq I_0,\ -\frac{k_j}{N_j} = \Re(s_0)\ \forall j \in J,\ \bigcap_{j \in J} E_j(\mathbb{Q}_p) \neq \bigcup_{J \subsetneq J' \subseteq I}\ \bigcap_{j' \in J'} E_{j'}(\mathbb{Q}_p)\Big\}.$$

Proof. As discussed in the proof of theorem 1.1.5, we can obtain a log-resolution

$$h : Y \to \mathrm{Spec}(\mathbb{Q}_p[X_1, \ldots, X_m])$$

of the pair $\big(\mathrm{Spec}(\mathbb{Q}_p[X_1, \ldots, X_m]), \mathrm{Spec}(\mathbb{Q}_p[X_1, \ldots, X_m]/(F))\big)$ by taking the composition

$$Y \xrightarrow{h_0} \mathrm{Proj}(\mathbb{Q}_p[X_1, \ldots, X_m]) \xrightarrow{pr} \mathrm{Spec}(\mathbb{Q}_p[X_1, \ldots, X_m]),$$

where

$$\mathrm{Proj}(\mathbb{Q}_p[X_1, \ldots, X_m]) \xrightarrow{pr} \mathrm{Spec}(\mathbb{Q}_p[X_1, \ldots, X_m])$$

is the "projection" map from the Proj construction. The numerical datum of h corresponding to proper transform (under h_0) of the exceptional divisor of pr is given by (n, m).

By Igusa's theorem, there exists a polynomial $A \in \mathbb{Z}_{(p)}[T]$ such that

$$Z_{F,p}(T) = \frac{A(T)}{(1 - p^{-m}T^n)\prod_{i \in I_0}(1 - p^{-k_i}T^{N_i})}$$

and thus

$$Z^*_{F,p}(T) = \frac{A(T)}{\prod_{i \in I_0}(1 - p^{-k_i}T^{N_i})}.$$

□

Remark 1.3.3. *Due to the projectivity of the E_i's, the bound in remark 1.2.3 can be strengthened to*

$$\max\left\{\#J \,:\, J \subseteq I_0,\ -\frac{k_j}{N_j} = \Re(s_0)\ \forall j \in J,\ \bigcap_{j\in J} E_j(\mathbb{Q}_p) \neq \bigcup_{J\subsetneq J'\subseteq I}\ \bigcap_{j'\in J'} E_{j'}(\mathbb{Q}_p)\right\} \leq m-1.$$

We can also prove an analogue of [VZG08, Theorem 2.7] for primitive local Igusa zeta functions.

Proposition 1.3.4. *Let $F(X_1,\ldots,X_m) \in \mathbb{Z}_p[X_1,\ldots,X_m]$ be a form with a non-trivial zero in $\mathbb{Z}_p^m$. Then*

$$\sigma_p^*(F) = -\operatorname{plct}_{\mathbb{Q}_p}(F).$$

Proof. It is enough to repeat the argument in the proof of [VZG08, Theorem 2.7] (in a neighborhood of a non-trivial zero of F in $\mathbb{Z}_p^m$) for $\zeta_{F,p}^*(s)$ in place of $\zeta_{F,p}(s)$. The details are left to the reader. □

The analogue of corollary 1.2.7 for primitive Igusa local zeta functions reads as follows.

Corollary 1.3.5. *Let $F \in \mathbb{Z}_p[X_1,\ldots,X_m]$ be a form with a non-trivial zero in $\mathbb{Z}_p^m$. Then*

$$\mu_p^m(\{\mathbf{x}\in\mathbb{Z}_p^m \,:\, \|\mathbf{x}\|_p = 1,\ |F(\mathbf{x})|_p = p^{-k}\}) \ll_{F,p} k^{\nu_p^*(F)-1} p^{\sigma_p^*(F)\cdot k} \quad \text{as } k\to\infty.$$

and

$$\mu_p^m(\{\mathbf{x}\in\mathbb{Z}_p^m \,:\, \|\mathbf{x}\|_p = 1,\ |F(\mathbf{x})|_p = p^{-k_l}\}) \gg_{F,p} k^{\nu_p^*(F)-1} p^{\sigma_p^*(F)\cdot k_l} \quad \text{as } l\to\infty$$

for some arithmetic progression $(k_l)_l$.

In the rest of the chapter, we prove our result on $\sigma^*(F)$ and $\nu^*(F)$ for multivariate ($m \geq 2$) decomposable forms $F \in \mathbb{Z}[X_1,\ldots,X_m]$, that is homogeneous polynomials that can be written as product of linear forms over an algebraic closure of $\mathbb{Q}$.

For a decomposable form $F = L_1^{r_1} \dots L_l^{r_l} \in \mathbb{Z}[X_1, \dots, X_m]$, with $L_1, \dots, L_l \in \mathbb{C}[X_1, \dots, X_m]$ linear forms with distinct support, we denote

$$\mathrm{rk}(F) := \mathrm{rk}(L_1, \dots, L_l), \tag{1.13}$$

$$\mathcal{L}(F) := \left\{ W \leq \mathbb{C}^n \,:\, \exists I \subseteq \{1, \dots, l\}, W = \bigcap_{i \in I} \{L_i = 0\} \right\} \tag{1.14}$$

and

$$q(F) := \max_{\substack{W \in \mathcal{L}(F) \\ W \notin \{0, \mathbb{C}^m\}}} \frac{\sum_{L_i \supseteq W} r_i}{\operatorname{codim} W}. \tag{1.15}$$

The fact that $\mathrm{rk}(F)$, $\mathcal{L}(F)$ and $q(F)$ do not depend on the choice of the factorization should be apparent.

Definition 1.3.6. *We say that a decomposable form $F \in \mathbb{Z}[X_1, \dots, X_m]$ of degree n is of finite type if*

$$\mathrm{vol}(F) := \mu_\infty^m(\{\mathbf{x} \in \mathbb{R}^m \,:\, |F(\mathbf{x})| \leq 1\}) < \infty$$

and strongly of finite type if

$$q(F) < \frac{n}{m}.$$

Lemma 1.3.7. *Let $F \in \mathbb{Z}[X_1, \dots, X_m]$ be a decomposable form of degree n.*

1. *If F is of finite type, then $n > m$.*
2. *If F is strongly of finite type, then F is of finite type.*
3. *If F is of finite type and the splitting field of F over $\mathbb{Q}$ is totally real, then F is strongly of finite type.*

Proof. All the three statements follow immediately from [Thu01, Proposition on page 771]. □

The fundamental assumption that we will need to impose later on in order to obtain the results we are aiming at on the S-part of decomposable forms (cf. chapter 4) is that the forms under consideration must be of finite type. The role of this condition will be clear in the next chapter.

Theorem 1.3.8. *Let $F \in \mathbb{Z}[X_1, \ldots, X_m]$ be a decomposable form and let p be a prime number such that F has a non-trivial zero in $\mathbb{Z}_p^m$. Then one has*

$$\sigma_p^*(F) = -\frac{1}{q(F)}, \qquad \nu_p^*(F) \leq \min\{\mathrm{rk}(F), m-1\}.$$

Proof. In [Tei08], Teitler described how to construct a log-resolution

$$h : Y \to \mathrm{Spec}(\mathbb{C}[X_1, \ldots, X_m])$$

of the pair $\big(\mathrm{Spec}(\mathbb{C}[X_1, \ldots, X_m]), \mathrm{Spec}(\mathbb{C}[X_1, \ldots, X_m]/(F))\big)$ (in the notation of Teitler's paper $Y := V_{\mathcal{L}(F)\setminus\{\mathbb{C}^m\}}$).

Each $W \in \mathcal{L}(F) \setminus \{\mathbb{C}^m\}$ is dominated by a unique smooth irreducible one codimensional divisor E_W in Y. The irreducible components of the normal crossing divisor associated to h are given by these divisors E_W for W ranging in all of $\mathcal{L}(F) \setminus \{\mathbb{C}^m\}$ (cf. [Tei08, Lemma 2.1]).

Therefore
$$\mathrm{lct}_{\mathbb{C}}(F) = \min_{\substack{W \in \mathcal{L}(F) \\ W \neq \mathbb{C}^m}} \frac{\mathrm{codim}\, W}{\sum_{L_i \supseteq W} r_i}. \tag{1.16}$$

If $\mathrm{rk}(F) < m$, then the expressions (1.15) and (1.16) agree and one has

$$\frac{1}{q(F)} = \mathrm{lct}_{\mathbb{C}}(F) \leq \frac{\mathrm{rk}(F)}{n} < \frac{m}{n},$$

which implies

$$\sigma_p^*(F) = \sigma_p(F) = -\frac{1}{q(F)}.$$

and

$$\nu_p^*(F) = \nu_p(F) \leq \mathrm{rk}(F),$$

the last inequality being an immediate consequence of Igusa's theorem (and the construction of log-resolutions in [Tei08]).

If $\mathrm{rk}(F) = m$, then the log-resolution is of the form considered in the proof of theorem 1.3.2 and one has

$$\frac{1}{q(F)} = \mathrm{plct}_{\mathbb{C}}(F).$$

Threfore

$$\sigma_p^*(F) = -\frac{1}{q(F)}$$

by proposition 1.3.4 and

$$\nu_p^*(F) \leq m - 1$$

by theorem 1.3.2 and remark 1.3.3.

□

Remark 1.3.9. *In* [Tei08], *Teitler also proved that the log-resolution that we have used in the proof of theorem 1.3.8 can be considerably refined. In fact, a "minimal" log-resolution also happens to exist. To a theoretical extent, this is not particularly important for us. However, as explained in* [Tei08], *using the minimal log-resolution in place of our "naïve" one may drastically decrease the computation complexity of a brute-force numerical computation of $q(F)$.*

Chapter 2

Pure and mixed power sums over $\mathbb{N}_\Sigma$

Let

$$\Sigma = \{q_1, \dots, q_s\} \quad (s \geq 1) \tag{2.1}$$

be a $\mathbb{Q}$-multiplicatively independent subset of $\mathbb{R}_{>1}$ (i.e. $\{\log q_1, \dots, \log q_s\}$ is a $\mathbb{Q}$-linearly independent subset of $\mathbb{R}_{>0}$). We denote

$$\mathbb{N}_\Sigma := \{q_1^{k_1} \dots q_s^{k_s} \, : \, (k_1, \dots, k_s) \in \mathbb{Z}_{\geq 0}^s\}. \tag{2.2}$$

For each $h \in \mathbb{N}_\Sigma$ the numbers $v_{q_1}(h), \dots, v_{q_s}(h) \in \mathbb{Z}_{\geq 0}$ are uniquely determined by the writing

$$h = q_1^{v_{q_1}(h)} \dots q_s^{v_{q_s}(h)}. \tag{2.3}$$

Note that if $S = \{p_1, \dots, p_s\}$ is a finite non-empty set of primes, then v_{p_i} is the usual p_i-adic valuation for all $i \in \{1, \dots, s\}$.

Let $\alpha, \alpha' \in \mathbb{R}_{>0}$, $\nu_1, \dots \nu_s \in \mathbb{Z}_{\geq 1}$ and $L \in \mathbb{R}_{>1}$. In this chapter we study the asymptotic behaviour, as $L \to \infty$, of sums of the form

$$\sum_{h \in \mathbb{N}_\Sigma} v_{q_1}(h)^{\nu_1 - 1} \dots v_{q_s}(h)^{\nu_s - 1} \min\{h^\alpha, L^{\alpha + \alpha'} h^{-\alpha'}\}. \tag{2.4}$$

We call a sum of this form a *pure* power sum over $\mathbb{N}_\Sigma$ if $\nu_1 = \cdots = \nu_s = 1$ and a *mixed* power sum otherwise. We are able to determine the asymptotic rate in general.

Theorem 2.0.1. *Let $\Sigma = \{q_1, \dots, q_s\}$ $(s \geq 1)$ be a $\mathbb{Q}$-multiplicatively independent subset of $\mathbb{R}_{>1}$, $\alpha, \alpha' \in \mathbb{R}_{>0}$ and $\nu_1, \dots, \nu_s \in \mathbb{Z}_{\geq 0}$. Then one has*

$$\sum_{h \in \mathbb{N}_\Sigma} v_{q_1}(h)^{\nu_1 - 1} \dots v_{q_s}(h)^{\nu_s - 1} \min\{h^\alpha, L^{\alpha+\alpha'} h^{-\alpha'}\} \asymp_{\Sigma,\alpha,\alpha',\nu_1,\dots,\nu_s} L^\alpha (\log L)^{\nu_1 + \dots + \nu_s - 1}$$

as $L \to \infty$.

In the pure case, we can describe the asymptotic behaviour in a much more precise way.

If $\Sigma = \{q\}$ for some $q \in \mathbb{R}_{>1}$, then it is easy to see that the limit

$$\lim_{L \to \infty} \frac{1}{L^\alpha} \sum_{h \in \mathbb{N}_{\{q\}}} \min\{h^\alpha, L^{\alpha+\alpha'} h^{-\alpha'}\} \tag{2.5}$$

does not exist. In fact, with an elementary computation, we can even determine the exact values of the lim inf and the lim sup.

Theorem 2.0.2. *Let $q \in \mathbb{R}_{>1}$ and $\alpha, \alpha' \in \mathbb{R}_{>0}$. One has*

$$\liminf_{L \to \infty} \frac{1}{L^\alpha} \sum_{h \in \mathbb{N}_{\{q\}}} \min\{h^\alpha, L^{\alpha+\alpha'} h^{-\alpha'}\} = \left(1 + \frac{\alpha}{\alpha'}\right) \frac{q^{\alpha\alpha'/(\alpha+\alpha')}}{q^\alpha - 1} \left(\frac{\alpha'}{\alpha} \frac{q^\alpha - 1}{q^{\alpha'} - 1}\right)^{\alpha/(\alpha+\alpha')}$$

and

$$\limsup_{L \to \infty} \frac{1}{L^\alpha} \sum_{h \in \mathbb{N}_{\{q\}}} \min\{h^\alpha, L^{\alpha+\alpha'} h^{-\alpha'}\} = \begin{cases} 1 - \frac{1}{q^\alpha - 1} + \frac{1}{q^{\alpha'} - 1} & \alpha \geq \alpha', \\ 1 - \frac{1}{q^{\alpha'} - 1} + \frac{1}{q^\alpha - 1} & \alpha \leq \alpha'. \end{cases}$$

If $s \geq 2$, then the situation becomes more interesting and requires more sophisticated tools. Using a result from equidistribution theory due to Everest ([Eve92]), we get in this case an exact asymptotics.

Theorem 2.0.3. *Let $\Sigma = \{q_1, \dots, q_s\}$ be a $\mathbb{Q}$-multiplicatively independent subset of $\mathbb{R}_{>1}$, $\alpha, \alpha' \in \mathbb{R}_{>0}$ and $\nu_1, \dots, \nu_s \in \mathbb{Z}_{\geq 0}$. Suppose $s \geq 2$. Then there exists a constant $c(\Sigma) > 0$ such that for any $\alpha, \alpha' \in \mathbb{R}_{>0}$ one has*

$$\sum_{h \in \mathbb{N}_\Sigma} \min\{h^\alpha, L^{\alpha+\alpha'} h^{-\alpha'}\} \sim c(\Sigma) \cdot \left(\frac{1}{\alpha} + \frac{1}{\alpha'}\right) L^\alpha (\log L)^{s-1} \quad \text{as } L \to \infty.$$

The chapter is organized as follows. In section 2.1 we prove a preliminary easy result from discrete calculus. In sections 2.2, 2.3 and 2.4 we prove theorems 2.0.2, 2.0.3 and 2.0.1 respectively. Finally, in section 2.5 we will apply the theory developed in the previous paragraphs to the description of the asymptotic behaviour of certain sums that will play a central role in the rest of the thesis.

2.1 A result from discrete calculus

In this section we prove an elementary result (proposition 2.1.3 below). Such a result can probably be found in many introductory books in discrete calculus. However, in order to save reader's time, we give here a self-contained proof.

Definition 2.1.1. *The (forward) difference operator* Δ *on the collection of function from* $\mathbb{Z}_{\geq 0}$ *to* $\mathbb{R}$ *is the operator transforming a function* $f : \mathbb{Z}_{\geq 0} \to \mathbb{R}$ *into the function* $\Delta f : \mathbb{Z}_{\geq 0} \to \mathbb{R}$ *defined by* $\Delta f(t) := f(t+1) - f(t)$.

Lemma 2.1.2 (Summation by parts)**.** *For any* $f, g : \mathbb{Z}_{\geq 0} \to \mathbb{R}$, $t_0, t_1 \in \mathbb{Z}_{\geq 0}$, $t_0 < t_1$, *we have*

$$\sum_{t=t_0}^{t_1} f(t)\Delta g(t) = \big(f(t_1)g(t_1+1) - f(t_0)g(t_0)\big) - \sum_{t=t_0}^{t_1-1} g(t+1)\Delta f(t).$$

Proof. A straightforward computation yields

$$\begin{aligned}
\sum_{t=t_0}^{t_1} f(t)\Delta g(t) &= \sum_{t=t_0}^{t_1} f(t)g(t+1) - \sum_{t=t_0}^{t_1} f(t)g(t) \\
&= \sum_{t=t_0}^{t_1} f(t+1)g(t+1) - \sum_{t=t_0}^{t_1} g(t+1)\Delta f(t) - \sum_{t=t_0}^{t_1} f(t)g(t) \\
&= \big(f(t_1+1)g(t_1+1) - f(t_0)g(t_0)\big) - \sum_{t=t_0}^{t_1} g(t+1)\Delta f(t) \\
&= \big(f(t_1)g(t_1+1) - f(t_0)g(t_0)\big) - \sum_{t=t_0}^{t_1-1} g(t+1)\Delta f(t).
\end{aligned}$$

□

Summation by parts is the only tool we need for the proof of the result we are aiming at.

Proposition 2.1.3. *Let $\beta \in \mathbb{R}_{>1}$, $\alpha \in \mathbb{R}_{>0}$, $r \in \mathbb{N}$. Then*

$$(a) \quad \sum_{t=0}^{T} \beta^{\alpha t} t^r = \frac{1}{\beta^\alpha - 1} \beta^{\alpha(T+1)} T^r + \mathcal{O}_{\alpha,\beta}(\beta^{\alpha(T+1)} T^{r-1}) \quad \text{as } T \to \infty,$$

$$(b) \quad \sum_{t=T}^{\infty} \beta^{-\alpha t} t^r = \frac{1}{\beta^\alpha - 1} \beta^{-\alpha(T+1)} T^r + \mathcal{O}_{\alpha,\beta}(\beta^{-\alpha(T+1)} T^{r-1}) \quad \text{as } T \to \infty.$$

Proof. (a) We proceed by induction on r. If $r = 0$, then

$$\sum_{t=0}^{T} \beta^{\alpha t} = \frac{\beta^{\alpha(T+1)} - 1}{\beta^\alpha - 1} = \frac{1}{\beta^\alpha - 1} \beta^{\alpha(T+1)} + \mathcal{O}_{\alpha,\beta}(1)$$

and the claim follows a fortiori.

Suppose $r > 0$. Then summation by parts gives us

$$\begin{aligned}\sum_{t=0}^{T} \beta^{\alpha t} t^r &= \frac{1}{\beta^\alpha - 1} \sum_{t=0}^{T} \Delta(\beta^{\alpha t}) t^r \\ &= \frac{1}{\beta^\alpha - 1} \left(\beta^{\alpha(T+1)} T^r - \beta^\alpha \cdot \sum_{t=0}^{T-1} \beta^{\alpha t} \Delta(t^r) \right).\end{aligned}$$

On the other hand $\Delta(t^r)$ is a polynomial of degree $r - 1$ in t, so by the induction hypothesis

$$\sum_{t=0}^{T-1} \beta^{\alpha t} \Delta(t^r) \asymp_{\alpha,\beta} \beta^{\alpha T} T^{r-1} \quad \text{as } T \to \infty.$$

Therefore

$$\begin{aligned}\sum_{t=0}^{T} \beta^{\alpha t} t^r &= \frac{1}{\beta^\alpha - 1} \left(\beta^{\alpha(T+1)} T^r - \beta^\alpha \cdot \sum_{t=0}^{T-1} \beta^{\alpha t} \Delta(t^r) \right) \\ &= \frac{1}{\beta^\alpha - 1} \beta^{\alpha(T+1)} T^r + \mathcal{O}_{\alpha,\beta}(\beta^{\alpha(T+1)} T^{r-1}).\end{aligned}$$

(b) The argument follows exactly the same lines as in (a), using induction and summation by parts. If $r = 0$, then

$$\sum_{t=T}^{\infty} \beta^{-\alpha t} = \frac{1}{1 - \beta^{-\alpha}} - \frac{1 - \beta^{-\alpha T}}{1 - \beta^{-\alpha}} = \frac{1}{\beta^\alpha - 1} \beta^{-\alpha(T+1)}$$

and the claim follows a fortiori.

Suppose $r > 0$. Then summation by part gives us

$$\sum_{t=T}^{Z} \beta^{-\alpha t} t^r = -\frac{1}{1-\beta^{-\alpha}} \sum_{t=T}^{Z} \Delta(\beta^{-\alpha t}) t^r$$
$$= -\frac{1}{1-\beta^{-\alpha}} \Big((\beta^{-\alpha(Z+1)} Z^r - \beta^{-\alpha T} T^r) - \beta^{-\alpha} \cdot \sum_{t=T}^{Z-1} \beta^{-\alpha t} \Delta(t^r) \Big)$$

for any $Z > T$.

Letting $Z \to \infty$ we get

$$\sum_{t=T}^{\infty} \beta^{-\alpha t} t^r = \frac{1}{1-\beta^{-\alpha}} \Big(-\beta^{-\alpha T} T^r - \beta^{-\alpha} \cdot \sum_{t=T}^{\infty} \beta^{-\alpha t} \Delta(t^r). \Big)$$

We can then conclude as in (a).

□

2.2 Pure power sums ($s = 1$)

Let $q \in \mathbb{R}_{>1}$. As already mentioned pure power sums over $\mathbb{N}_{\{q\}}$ do not admit an exact asymptotics.

A straightforward computation shows that for any $\alpha, \alpha' \in \mathbb{R}_{>0}$ one has

$$\sum_{\substack{h \in \mathbb{N}_{\{q\}} \\ h \le L}} h^{\alpha} = \sum_{k=0}^{\lfloor \log_q L \rfloor} q^{k\alpha} = \frac{q^{\alpha(\lfloor \log_q L \rfloor + 1)} - 1}{q^{\alpha} - 1} \tag{2.6}$$

and thus

$$\sum_{\substack{h \in \mathbb{N}_{\{q\}} \\ h \le L}} h^{\alpha} = \frac{q^{\alpha(1 - \{\log_q L\})}}{q^{\alpha} - 1} L^{\alpha} + \mathcal{O}_{q,\alpha}(1) \quad \text{as } L \to \infty. \tag{2.7}$$

Also, for any $L \in \mathbb{R}_{>1}$ one has

$$\sum_{\substack{h \in \mathbb{N}_{\{q\}} \\ h > L}} h^{-\alpha'} = \sum_{k=\lfloor \log_q L \rfloor + 1}^{\infty} q^{-k\alpha'} = \frac{1}{1-q^{-\alpha'}} - \frac{1 - q^{-\alpha'(\lfloor \log_q L \rfloor + 1)}}{1 - q^{-\alpha'}} \tag{2.8}$$

and thus

$$\sum_{\substack{h\in\mathbb{N}_{\{q\}}\\ h>L}} h^{-\alpha'} = \frac{q^{-\alpha'(\lfloor \log_q L\rfloor+1)}}{1-q^{-\alpha'}} = \frac{q^{\alpha'\{\log_q L\}}}{q^{\alpha'}-1} L^{-\alpha'} \quad \forall L\in\mathbb{R}_{>1}\,. \tag{2.9}$$

Summing (2.8) and (2.9), we obtain

$$\sum_{h\in\mathbb{N}_{\{q\}}} \min\{h^\alpha, L^{\alpha+\alpha'}h^{-\alpha'}\} = \left(\frac{q^{\alpha(1-\{\log_p L\})}}{q^\alpha-1} + \frac{q^{\alpha'\{\log_q L\}}}{q^{\alpha'}-1}\right)L^\alpha + \mathcal{O}_{q,\alpha,\alpha'}(1) \tag{2.10}$$

as $L\to\infty$.

Now, since the map $\mathbb{R}\to[0,1)$, $L\mapsto\{\log_q L\}$ is clearly surjective, we deduce from (2.10) that

$$\liminf_{L\to\infty}\frac{1}{L^\alpha}\sum_{h\in\mathbb{N}_{\{q\}}} \min\{h^\alpha, L^{\alpha+\alpha'}h^{-\alpha'}\} = \inf_{u\in[0,1)}\mathcal{L}(u) \tag{2.11}$$

and

$$\limsup_{L\to\infty}\frac{1}{L^\alpha}\sum_{h\in\mathbb{N}_{\{q\}}} \min\{h^\alpha, L^{\alpha+\alpha'}h^{-\alpha'}\} = \sup_{u\in[0,1)}\mathcal{L}(u). \tag{2.12}$$

where $\mathcal{L}:\mathbb{R}\to(0,\infty)$ is defined by

$$\mathcal{L}(u) := \frac{A^{1-u}}{A-1} + \frac{A^{\rho u}}{A^\rho-1} \qquad (A := q^\alpha,\ \rho := \alpha'/\alpha). \tag{2.13}$$

Theorem 2.0.2 follows then from the following result on the function $\mathcal{L}$.

Lemma 2.2.1. *In the notation above, one has*

$$(a)\qquad \inf_{u\in[0,1)}\mathcal{L}(u) = \left(1+\frac{1}{\rho}\right)\frac{A}{A-1}A^{-1/(1+\rho)}\left(\frac{\rho(A-1)}{A^\rho-1}\right)^{1/(1+\rho)},$$

$$(b)\qquad \sup_{u\in[0,1)}\mathcal{L}(u) = \begin{cases} 1-\frac{1}{A-1}+\frac{1}{A^\rho-1} & \text{if } \rho\le 1,\\ 1-\frac{1}{A^\rho-1}+\frac{1}{A-1} & \text{if } \rho\ge 1.\end{cases}$$

Proof. The function $\mathcal{L}$ is convex, so it has a unique stationary point $u^*\in\mathbb{R}$, at which $\mathcal{L}$ assumes its global minimum over $\mathbb{R}$. A straightforward computation shows that

$$u^* = \frac{1}{\alpha(1+\rho)}\left(\alpha - \log_q\left(\frac{\rho(A-1)}{A^\rho-1}\right)\right).$$

If we consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = 1 - A^{-x} - x(A-1) \quad (x \in \mathbb{R}).$$

then we see that

$$f'(x) = (\log A)\left(A^{-x} - \frac{A-1}{\log A}\right) < 0 \quad \forall x > 0,$$

which implies

$$1 - A^{-\rho} - \rho(A-1) = f(\rho) < f(0) = 0,$$

and thus

$$\frac{\rho(A-1)}{A^{\rho}-1} > A^{-\rho},$$

This proves that

$$u^* < 1. \tag{2.14}$$

Similarly, for the function $g : \mathbb{R} \to \mathbb{R}$ defined by

$$g(x) = A(A^x - 1) - x(A-1) \quad (x \in \mathbb{R}),$$

we compute

$$g'(x) = (\log A)\left(A^{1+x} - \frac{A-1}{\log A}\right) > 0 \quad \forall x > 0,$$

from which we deduce

$$A(A^{\gamma} - 1) - \gamma(A-1) = g(\gamma) > g(0) = 0$$

and thus

$$\frac{\gamma(A-1)}{A^{\gamma}-1} < A.$$

This gives us

$$u^* > 0. \tag{2.15}$$

From (2.14) and (2.15), we conclude that

$$u^* \in (0,1),$$

which implies

$$\inf_{u\in[0,1)} \mathcal{L}(u) = \mathcal{L}(u^*) \tag{2.16}$$

and

$$\sup_{u\in[0,1)} \mathcal{L}(u) = \max\{\mathcal{L}(0), \mathcal{L}(1)\}. \tag{2.17}$$

The claims (a) and (b) in the lemma follow from 2.16 (by evaluating $\mathcal{L}$ at the u^*) and from 2.17 (by evaluating $\mathcal{L}$ at 0 and 1) respectively. □

2.3 Pure power sums ($s \geq 2$)

In this section we consider pure power sums over $\mathbb{N}_\Sigma$ in the case $s \geq 2$. The key ingredient in the proof of theorem 2.0.3 is the study of the asymptotic behaviour, as $t \to \infty$, of the number of integer points in the regions of $\mathbb{R}^s$ defined as follows.

Definition 2.3.1. *Let $\Sigma = \{q_1, \ldots, q_s\}$ be a $\mathbb{Q}$-multiplicatively independent subset of $\mathbb{R}_{\geq 1}$ with $s \geq 2$. For any $\beta \in \mathbb{R}_{>1}$, $t \in \mathbb{Z}_{\geq 0}$, we define*

$$\mathcal{M}_t^\beta(\Sigma) := \left\{ \mathbf{x} \in \mathbb{R}^s \;:\; \begin{array}{c} x_i \geq 0 \quad \forall i \in \{1, \ldots, s\}, \\ t < x_1 \log_\beta q_1 + \cdots + x_s \log_\beta q_s \leq t+1 \end{array} \right\}.$$

If $\beta = e$, then we drop the superscript.

These regions give rise to a partition

$$\mathbb{N}_\Sigma \setminus \{1\} = \bigcup_{t=0}^{\infty} \{h \in \mathbb{N}_\Sigma \;:\; (v_{q_1}(h), \ldots, v_{q_s}(h)) \in \mathcal{M}_t^\beta(\Sigma)\}, \tag{2.18}$$

according to which we may split the pure power sums under consideration.

Note that the partition (2.18) becomes finer and finer as $\beta \to 1^+$. Moreover, the ratio between the maximum and the minimum of the summand on each $\mathcal{M}_t^\beta(\Sigma)$ tends to 1 as $\beta \to 1^+$. Therefore we expect that the estimates (for fixed β) on the sums we are considering would yield, in the limit $\beta \to 1^+$, a precise description of the asymptotic behaviour.

Lemma 2.3.2. *Let $\Sigma = \{q_1, \dots, q_s\}$ be a $\mathbb{Q}$-multiplicatively independent subset of $\mathbb{R}_{\geq 1}$ with $s \geq 2$. Then there exists a constant $c(\Sigma) \in \mathbb{R}_{>0}$ such that for any $\beta \in \mathbb{R}_{>1}$ one has*

$$\#(\mathbb{Z}^s \cap \mathcal{M}_t^\beta(\Sigma)) = c(\Sigma) \cdot (\log \beta)^s t^{s-1} + o_\beta(t^{s-1}) \quad \text{as } t \to \infty.$$

Proof. Let

$$\mathcal{B}_t^\beta(\Sigma) := \left\{ \mathbf{x} \in \mathbb{R}^s : \begin{array}{c} x_i \geq 0 \quad \forall i \in \{1, \dots, s\}, \\ x_1 \log_\beta q_1 + \dots + x_s \log_\beta q_s \leq t \end{array} \right\}. \tag{2.19}$$

From [Eve92, Theorem 1], it follows that there exist constants $c'(\Sigma), c''(\Sigma) \in \mathbb{R}_{>0}$ such that for any $\beta \in \mathbb{R}_{>1}$ one has

$$\#(\mathbb{Z}^s \cap \mathcal{B}_t^\beta(\Sigma)) = c'(\Sigma) \cdot (\log \beta)^s t^s + c''(\Sigma) \cdot (\log \beta)^{s-1} t^{s-1} + o_\beta(t^{s-1})$$

as $t \to \infty$.

The claim follows then, with $c(\Sigma) := c'(\Sigma) \cdot s$, from the fact that $\mathcal{M}_t^\beta(\Sigma) = \mathcal{B}_{t+1}^\beta(\Sigma) \setminus \mathcal{B}_t^\beta(\Sigma)$ for all $t \in \mathbb{Z}_{\geq 0}$ (clear from (2.19)). □

Theorem 2.0.3 follows immediately from the following proposition.

Proposition 2.3.3. *Let $\Sigma = \{q_1, \dots, q_s\}$ be a $\mathbb{Q}$-multiplicatively independent subset of $\mathbb{R}_{\geq 1}$ with $s \geq 2$. For any $\alpha \in \mathbb{R}_{>0}$ one has*

$$(a) \quad \sum_{\substack{h \in \mathbb{N}_\Sigma \\ h \leq L}} h^\alpha \sim \frac{c(\Sigma)}{\alpha} L^\alpha (\log L)^{s-1} \quad \text{as } L \to \infty,$$

$$(b) \quad \sum_{\substack{h \in \mathbb{N}_\Sigma \\ h > L}} h^{-\alpha} \sim \frac{c(\Sigma)}{\alpha} L^{-\alpha} (\log L)^{s-1} \quad \text{as } L \to \infty.$$

Proof. (a) Estimating every $h \in \mathbb{N}_\Sigma$ such that $\log_\beta h \in \mathcal{M}_t^\beta(\Sigma)$ (with any $t \in \mathbb{Z}_{\geq 0}$) with β^t from below and with β^{t+1} from above, proposition 2.1.3(a) yields

$$\begin{aligned}
\sum_{\substack{h\in\mathbb{N}_\Sigma\\ h\le L}} h^\alpha &\le 1 + \sum_{t=0}^{\lceil \log_\beta L\rceil -1} \beta^{\alpha(t+1)} \cdot \#(\mathbb{Z}^s \cap \mathcal{M}_t^\beta(\Sigma)) \\
&= 1 + \sum_{t=0}^{\lceil \log_\beta L\rceil -1} \beta^{\alpha(t+1)} \cdot \left(c(\Sigma)\cdot(\log\beta)^s t^{s-1} + o_{\alpha,\beta}(t^{s-1})\right) \\
&= c(\Sigma)\cdot(\log\beta)^s \left(\sum_{t=0}^{\lceil \log_\beta L\rceil -1} \beta^{\alpha(t+1)} t^{s-1}\right) + o_{\alpha,\beta}(L^\alpha(\log L)^{s-1}) \\
&= \frac{c(\Sigma)(\log\beta)^s}{\beta^\alpha - 1}\cdot \beta^{\alpha(1+\lceil \log_\beta L\rceil)}(\log_\beta L)^{s-1} + o_{\alpha,\beta}(L^\alpha(\log L)^{s-1}) \\
&\le \frac{\beta^{2\alpha}\log\beta}{\beta^\alpha-1}\cdot c(\Sigma)\cdot L^\alpha(\log L)^{s-1} + o_{\alpha,\beta}(L^\alpha(\log L)^{s-1})
\end{aligned}$$

and thus

$$\limsup_{L\to\infty} \frac{1}{L^\alpha(\log L)^{s-1}} \sum_{\substack{h\in\mathbb{N}_\Sigma\\ h\le L}} h^\alpha \le c(\Sigma)\cdot \lim_{\beta\to 1^+} \frac{\beta^{2\alpha}\log\beta}{\beta^\alpha-1} = \frac{c(\Sigma)}{\alpha}.$$

Similarly

$$\begin{aligned}
\sum_{\substack{h\in\mathbb{N}_\Sigma\\ h\le L}} h^\alpha &\ge \sum_{t=0}^{\lfloor \log_\beta L\rfloor -1} \beta^{\alpha t} \cdot \#(\mathbb{Z}^s \cap \mathcal{M}_t^\beta(\Sigma)) \\
&\ge \frac{\log\beta}{\beta^{2\alpha}(\beta^\alpha-1)}\cdot c(\Sigma)\cdot L^\alpha(\log L)^{s-1} + o_\beta(L^\alpha(\log L)^{s-1})
\end{aligned}$$

and thus

$$\liminf_{L\to\infty} \frac{1}{L^\alpha(\log L)^{s-1}} \sum_{\substack{h\in\mathbb{N}_\Sigma\\ h\le L}} h^\alpha \ge c(\Sigma)\cdot \lim_{\beta\to 1^+} \frac{\log\beta}{\beta^{2\alpha}(\beta^\alpha-1)} = \frac{c(\Sigma)}{\alpha}.$$

(b) The proof follows exactly the same lines as (a), using 2.1.3(b) in place of 2.1.3(a).

□

2.4 Mixed power sums

In order to prove our claim for mixed power sums, we need a deeper insight in the distribution of integer points in the sets $\mathcal{M}_t(\Sigma)$ as $t \to \infty$. In fact, the key idea in the proof of theorem 2.0.1 in the mixed case is noticing that, as $t \to \infty$, the points $\mathbf{k} = (k_1, \dots, k_s)$ with integer coordinates tend to distribute inside $\mathcal{M}_t(\Sigma)$ in such a way that the quantities $k_i \log q_i$ $(i = 1, \dots, s)$ all grow with order t. Lemma 2.4.2 below formalizes this idea.

Definition 2.4.1. *Let $\Sigma = \{q_1, \dots, q_s\}$ be a $\mathbb{Q}$-multiplicatively independent subset of $\mathbb{R}_{>1}$ with $s \geq 2$. For any function $\omega : [0, \infty) \to [0, \infty)$ and any $t \in \mathbb{Z}_{\geq 0}$, we define*

$$\mathcal{M}_t(\Sigma, \omega) := \left\{ \mathbf{x} \in \mathbb{R}^s \ : \ \begin{array}{c} x_i \geq \omega(t)/\log q_i \quad \forall i \in \{1, \dots, s\}, \\ t < x_1 \log q_1 + \dots + x_s \log q_s \leq t+1 \end{array} \right\}.$$

Lemma 2.4.2. *Let $\Sigma = \{q_1, \dots, q_s\}$ be a $\mathbb{Q}$-multiplicatively independent subset of $\mathbb{R}_{>1}$ with $s \geq 2$. Suppose that $\omega : [0, \infty) \to [0, \infty)$ satisfies*

$$\limsup_{t \to \infty} \frac{\omega(t)}{t} < c(\Sigma) \cdot \left(\sum_{j=1}^{s} \frac{c(\Sigma \setminus \{q_j\})}{\log q_j} \right)^{-1},$$

where $c(\Sigma)$ is the constant that appears in lemma 2.3.2 if $s > 1$ and

$$c(\{q\}) := 1 + \frac{1}{\log q} \quad \forall q \in \mathbb{R}_{\geq 1}.$$

Then one has

$$\#(\mathbb{Z}^s \cap \mathcal{M}_t(\Sigma, \omega)) \asymp_{\Sigma, \omega} t^{s-1} \quad \text{as } t \to \infty.$$

Proof. Clearly $\#(\mathbb{Z}^s \cap \mathcal{M}_t(\Sigma, \omega)) \leq \#(\mathbb{Z}^s \cap \mathcal{M}_t(\Sigma, \omega)) \ll_{\Sigma, \omega} t^{s-1}$ as $t \to \infty$. We want to prove that one also has

$$\liminf_{t \to \infty} \frac{\#(\mathbb{Z}^s \cap \mathcal{M}_t(\Sigma, \omega))}{t^{s-1}} > 0.$$

Since

$$\begin{aligned}
&\liminf_{t\to\infty}\frac{\#(\mathbb{Z}^s\cap\mathcal{M}_t(\Sigma,\omega))}{t^{s-1}}\\
&\qquad\geq \lim_{t\to\infty}\frac{\#(\mathbb{Z}^s\cap\mathcal{M}_t(\Sigma))}{t^{s-1}}-\limsup_{t\to\infty}\frac{\#(\mathbb{Z}^s\cap(\mathcal{M}_t(\Sigma)\setminus\mathcal{M}_t(\Sigma,\omega)))}{t^{s-1}}\\
&\qquad= c(\Sigma)-\limsup_{t\to\infty}\frac{\#(\mathbb{Z}^s\cap(\mathcal{M}_t(\Sigma)\setminus\mathcal{M}_t(\Sigma,\omega)))}{t^{s-1}},
\end{aligned}$$

it is enough to show that

$$\limsup_{t\to\infty}\frac{\#(\mathbb{Z}^s\cap(\mathcal{M}_t(\Sigma)\setminus\mathcal{M}_t(\Sigma,\omega)))}{t^{s-1}}<c(\Sigma).$$

Write

$$\mathbb{Z}^s\cap(\mathcal{M}_t(\Sigma)\setminus\mathcal{M}_t(\Sigma,\omega))=\bigcup_{j=1}^{s}\ \bigcup_{k_j=0}^{\lceil\omega(t)/\log q\rceil-1}\mathbb{Z}^s\cap\mathcal{A}_{t,j}(k_j),$$

with

$$\mathcal{A}_{t,j}(k_j):=\left\{x\in\mathbb{R}^s\ :\ \begin{array}{c} x_i\geq 0\,\forall i,\ x_j=k_j,\\ t-k_j\log q_j<\sum_{i\neq j}x_i\log q_i\leq t+1-k_j\log q_j\end{array}\right\}.$$

If $s=2$, then

$$\#(\mathbb{Z}^2\cap\mathcal{A}_{t,1}(k_1))\leq 1+\frac{1}{\log q_2}\quad\text{and}\quad\#(\mathbb{Z}^2\cap\mathcal{A}_{t,2}(k_2))\leq 1+\frac{1}{\log q_1}$$

for all $k_1\in\{0,\dots,\lceil\omega(t)/\log q_1\rceil-1\}$, $k_2\in\{0,\dots,\lceil\omega(t)/\log q_2\rceil-1\}$, from which it follows that

$$\begin{aligned}
&\#(\mathbb{Z}^2\cap(\mathcal{M}_t(\Sigma)\setminus\mathcal{M}_t(\Sigma,\omega)))\\
&\qquad\leq\sum_{j=1}^{2}\ \sum_{k_j=0}^{\lceil\omega(t)/\log q_j\rceil-1}\#(\mathbb{Z}^s\cap\mathcal{A}_{t,j}(k_j))\\
&\qquad\leq\Big(1+\frac{1}{\log q_1}\Big)\Big(\frac{\omega(t)}{\log q_2}+1\Big)+\Big(1+\frac{1}{\log q_2}\Big)\Big(\frac{\omega(t)}{\log q_1}+1\Big)\\
&\qquad=\Big(\frac{1}{\log q_1}+\frac{1}{\log q_2}+\frac{2}{(\log q_1)(\log q_2)}\Big)\,\omega(t)+\Big(2+\frac{1}{\log q_1}+\frac{1}{\log q_2}\Big)
\end{aligned}$$

and thus

$$\begin{aligned}\limsup_{t\to\infty}&\frac{\#(\mathbb{Z}^2\cap(\mathcal{M}_t(\Sigma)\setminus\mathcal{M}_t(\Sigma,\omega)))}{t}\\ &=\Big(\frac{1}{\log q_1}+\frac{1}{\log q_2}+\frac{2}{(\log q_1)(\log q_2)}\Big)\limsup_{t\to\infty}\frac{\omega(t)}{t}\\ &< c(\Sigma).\end{aligned}$$

Suppose now $s\geq 3$. Then $s-1\geq 2$ and so

$$\#(\mathbb{Z}^s\cap\mathcal{A}_{t,j}(k_j))=c(\Sigma\setminus\{q_j\})\cdot t^{s-2}+o_\Sigma(t^{s-2})\quad \text{as } t\to\infty$$

by lemma 2.3.2.

It follows that

$$\begin{aligned}\limsup_{t\to\infty}\frac{\mathbb{Z}^s\cap(\mathcal{M}_t(\Sigma)\setminus\mathcal{M}_t(\Sigma,\omega))}{t^{s-1}}&\leq\Big(\sum_{j=1}^{s}\frac{c(\Sigma\setminus\{q_j\})}{\log q_j}\Big)\limsup_{t\to\infty}\frac{\omega(t)}{t}\\ &< c(\Sigma).\end{aligned}$$

□

We need now the following easy technical lemma.

Lemma 2.4.3. *Let $f,g:(0,\infty)\to(0,\infty)$ be two functions, with $f(t)\ll g(t)$ as $t\to\infty$. Suppose that there exists $c>0$ such that $f(t)\gg\xi(t)$ as $t\to\infty$ for all functions $\xi:(0,\infty)\to(0,\infty)$ satisfying*

$$\liminf_{t\to\infty}\frac{\xi(t)}{g(t)}=0\quad\textit{and}\quad\limsup_{t\to\infty}\frac{\xi(t)}{g(t)}<c.$$

Then one has

$$f(t)\asymp g(t)\quad \textit{as } t\to\infty.$$

Proof. Let

$$l:=\liminf_{t\to\infty}\frac{f(t)}{g(t)},\quad L:=\limsup_{t\to\infty}\frac{f(t)}{g(t)}.$$

Since by assumption $L < \infty$, we only need to prove that $l > 0$.

We show first that $L > 0$. If by contradiction $L = 0$, then for

$$\xi_0 \,:\, (0,\infty) \to (0,\infty), \quad t \mapsto (f(t)g(t))^{1/2}$$

we see that

$$\lim_{t\to\infty} \frac{\xi_0(t)}{g(t)} = \lim_{t\to\infty} \left(\frac{f(t)}{g(t)}\right)^{1/2} = 0$$

and

$$\limsup_{t\to\infty} \frac{\xi_0(t)}{f(t)} = \limsup_{t\to\infty} \left(\frac{g(t)}{f(t)}\right)^{1/2} = \infty,$$

which contradicts our assumptions.

Now, suppose by contradiction that $l = 0$. Because $L > 0$, we may consider the function

$$\xi \,:\, (0,\infty) \to (0,\infty), \quad t \mapsto \frac{c}{2L^{1/2}}(f(t)g(t))^{1/2}.$$

Since

$$\liminf_{t\to\infty} \frac{\xi(t)}{g(t)} = \frac{c}{2L^{1/2}} \liminf_{t\to\infty} \left(\frac{f(t)}{g(t)}\right)^{1/2} = 0,$$

$$\limsup_{t\to\infty} \frac{\xi(t)}{g(t)} = \frac{c}{2L^{1/2}} \limsup_{t\to\infty} \left(\frac{f(t)}{g(t)}\right)^{1/2} = \frac{c}{2} < c$$

and

$$\limsup_{t\to\infty} \frac{\xi(t)}{f(t)} = \frac{c}{2L^{1/2}} \limsup_{t\to\infty} \left(\frac{g(t)}{f(t)}\right)^{1/2} = \infty,$$

we reach a contradiction. □

Lemma 2.4.4. *Let $\Sigma = \{q_1,\dots,q_s\}$ $(s \geq 2)$ be a multiplicatively independent subset of $\mathbb{R}_{>1}$ and $\nu_1,\dots\nu_s \in \mathbb{Z}_{\geq 1}$. Suppose that $\nu_1 + \cdots + \nu_s > s$. Then*

$$\sum_{\mathbf{k}\in\mathbb{Z}^s \cap \mathcal{M}_t(\Sigma)} k_1^{\nu_1-1} \dots k_s^{\nu_s-1} \asymp_{\Sigma,\nu_1,\dots,\nu_s} t^{\nu_1+\cdots+\nu_s-1} \quad \text{as } t \to \infty.$$

Proof. By the inequality between the arithmetic and the geometric mean and by lemma 2.4.2, we have

$$\begin{aligned}
&\sum_{\mathbf{k}\in\mathbb{Z}^s\cap\mathcal{M}_t(\Sigma)} k_1^{\nu_1-1}\dots k_s^{\nu_s-1}\\
&= \frac{1}{(\log q_1)^{\nu_1-1}\dots(\log q_s)^{\nu_s-1}} \sum_{\mathbf{k}\in\mathbb{Z}^s\cap\mathcal{M}_t} (k_1\log q_1)^{\nu_1-1}\dots(k_s\log q_s)^{\nu_s-1}\\
&\leq \left(\prod_{i=1}^{s}\frac{1}{(\log q_i)^{\nu_i-1}}\right)\left(\frac{\max_i \nu_i - 1}{\nu_1+\dots+\nu_s-s}\right)^{\nu_1+\dots+\nu_s}(t+1)^{\nu_1+\dots+\nu_s-s}\#(\mathbb{Z}^s\cap\mathcal{M}_t(\Sigma))\\
&\ll_{\Sigma,\nu_1,\dots,\nu_s} t^{\nu_1+\dots+\nu_s-1} \quad \text{as } t\to\infty,
\end{aligned}$$

from which the upper bound follows.

Now, let $\xi:(0,\infty)\to(0,\infty)$ be any function such that

$$\liminf_{t\to\infty}\frac{\xi(t)}{t^{\nu_1+\dots+\nu_s-1}} = 0$$

and

$$\limsup_{t\to\infty}\frac{\xi(t)}{t^{\nu_1+\dots+\nu_s-1}} < \left(c(\Sigma)\cdot\left(\sum_{j=1}^{s}\frac{c(\Sigma\setminus\{q_j\})}{\log q_j}\right)^{-1}\right)^{\nu_1+\dots+\nu_s-s}.$$

We consider the function $\omega:(0,\infty)\to(0,\infty)$ defined by

$$\omega(t) := \left(\frac{\xi(t)}{t^{s-1}}\right)^{1/(\nu_1+\dots+\nu_s-s)}.$$

Since

$$\limsup_{t\to\infty}\frac{\omega(t)}{t} = \left(\limsup_{t\to\infty}\frac{\xi(t)}{t}\right)^{1/(\nu_1+\dots+\nu_s-s)} < c(\Sigma)\cdot\left(\sum_{j=1}^{s}\frac{c(\Sigma\setminus\{q_j\})}{\log q_j}\right)^{-1},$$

lemma 2.4.2 tells us that

$$\begin{aligned}
\sum_{\mathbf{k}\in\mathbb{Z}^s\cap\mathcal{M}_t(\Sigma)} k_1^{\nu_1-1}\dots k_s^{\nu_s-1} &\geq \sum_{k\in\mathbb{Z}^s\cap\mathcal{M}_t(\Sigma,\omega)} k_1^{\nu_1-1}\dots k_s^{\nu_s-1}\\
&\geq \frac{\omega(t)^{\nu_1+\dots+\nu_s-s}}{(\log q_1)^{\nu_1-1}\dots(\log q_s)^{\nu_s-1}}\cdot\#(\mathbb{Z}^s\cap\mathcal{M}_t(\Sigma,\omega))\\
&\gg_{\Sigma,\nu_1,\dots,\nu_s} (\log\beta)^{\nu_1+\dots+\nu_s}\xi(t) \quad \text{as } t\to\infty.
\end{aligned}$$

The desired lower bound follows then from lemma 2.4.3. □

Theorem 2.0.1 follows immediately from the following proposition.

Proposition 2.4.5. *Let* $\Sigma = \{q_1, \ldots, q_s\}$ $(s \geq 1)$ *be a multiplicatively independent subset of* $\mathbb{R}_{>1}$*,* $\alpha \in \mathbb{R}_{>0}$ *and* $\nu_1, \ldots, \nu_s \in \mathbb{Z}_{\geq 1}$*. Then one has*

$$(a) \quad \sum_{\substack{h \in \mathbb{N}_\Sigma \\ h \leq L}} v_{q_1}(h)^{\nu_1 - 1} \ldots v_{q_s}(h)^{\nu_s - 1} h^{\alpha} \asymp L^{\alpha} (\log L)^{\nu_1 + \cdots + \nu_s - 1} \quad \text{as } L \to \infty,$$

$$(b) \quad \sum_{\substack{h \in \mathbb{N}_\Sigma \\ h > L}} v_{q_1}(h)^{\nu_1 - 1} \ldots v_{q_s}(h)^{\nu_s - 1} h^{-\alpha} \asymp L^{-\alpha} (\log L)^{\nu_1 + \cdots + \nu_s - 1} \quad \text{as } L \to \infty.$$

Proof. If $s = 1$, then the claim follows immediately from proposition 2.1.3.

If $s \geq 2$ and $\nu_i = 1 \, \forall i \in \{1, \ldots, s\}$, then the result is just a weak version of theorem 2.3.3.

If $s \geq 2$ and $\nu_1 + \cdots + \nu_s > s$, then the proof of the claim follows the same line as that of theorem 2.3.3, using lemma 2.4.4 in place of lemma 2.3.2. □

2.5 Applications

In this section, we apply the results obtained above to the study of the asymptotic behaviour of certain sums that will play important roles in the next chapters.

Recall that, for any $f \in \mathbb{R}[X_1, \ldots, X_m]$ and $B, M \in \mathbb{R}_{>0}$, we denote

$$V_f(B, M) := \{\mathbf{x} \in \mathbb{R}^m \, : \, |f(\mathbf{x})| \leq M\}. \tag{2.20}$$

Definition 2.5.1. *Let* $f \in \mathbb{Z}[X]$*,* $B, \gamma, \varepsilon \in \mathbb{R}_{>0}$*,* $\sigma \in \mathbb{R}_{<0}$ *and let* $\Sigma = \{q_1, \ldots, q_s\}$ *be a* $\mathbb{Q}$*-multiplicative independent subset of* $\mathbb{R}_{>1}$*. We define*

$$U(f, \Sigma, \varepsilon, B, \gamma, \sigma) := \sum_{h \in \mathbb{N}_\Sigma} \mu_\infty(V_f(B, (\gamma h)^{1/\varepsilon})) \cdot h^{\sigma}$$

The results from section 2.3, together with a careful use of the polynomial growth, lead us to the following precise description of the asymptotic behaviour of $U(f,S,\varepsilon,B,\gamma,\sigma)$ as $B\to\infty$.

Definition 2.5.2. *For $q\in\mathbb{R}_{>1}$, $\varepsilon\in\mathbb{R}_{>0}$, $\sigma\in\mathbb{R}_{<0}$, we denote*

$$(a)\quad \lambda^-(n,\sigma,q,\varepsilon) := -\frac{1}{\sigma n\varepsilon}\frac{q^{-\sigma(1+\sigma n\varepsilon)}}{q^{1/(n\varepsilon)+\sigma}-1}\Big(-\frac{\sigma}{1/(n\varepsilon)+\sigma}\frac{q^{1/(n\varepsilon)+\sigma}-1}{q^{-\sigma}-1}\Big)^{1+\sigma n\varepsilon},$$

$$(b)\quad \lambda^+(n,\sigma,q,\varepsilon) := \begin{cases} 1-\frac{1}{q^{1/(n\varepsilon)+\sigma}-1}+\frac{1}{q^{-\sigma}-1} & \varepsilon\le -\frac{1}{2\sigma n},\\ 1-\frac{1}{q^{-\sigma}-1}+\frac{1}{q^{1/(n\varepsilon)+\sigma}-1} & \varepsilon\ge -\frac{1}{2\sigma n}.\end{cases}$$

Proposition 2.5.3. *Let $f\in\mathbb{Z}[X]$ be a polynomial of degree $n\ge 1$ and leading coefficient c_f. Let also $\gamma\in\mathbb{R}_{>0}$, $\sigma\in\mathbb{R}_{<0}$, $\varepsilon\in\left(0,-\frac{1}{n\sigma}\right)$ and let $\Sigma=\{q_1,\dots,q_s\}$ $(s\ge 1)$ be a $\mathbb{Q}$-multiplicative independent subset of $\mathbb{R}_{>1}$.*

(a) If $\Sigma=\{q\}$, then one has

$$\liminf_{B\to\infty}\frac{U(f,\{q\},\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}} = \lambda^-(n,\sigma,q,\varepsilon)\cdot|c_f|^{\sigma\varepsilon}\gamma^{-\sigma},$$
$$\limsup_{B\to\infty}\frac{U(f,\{q\},\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}} = \lambda^+(n,\sigma,q,\varepsilon)\cdot|c_f|^{\sigma\varepsilon}\gamma^{-\sigma}.$$

(b) If $s\ge 2$, then

$$U(f,\Sigma,\varepsilon,B,\gamma,\sigma)\sim 2\cdot c(S)\cdot\frac{|c_f|^{\sigma\varepsilon}\gamma^{-\sigma}}{-\sigma(1+\sigma n\varepsilon)}\cdot B^{1+\sigma n\varepsilon}(\log B)^{s-1}\quad \textit{as } B\to\infty.$$

Proof. For any $\delta\in(0,1/2)$ there exists $B_\delta>1$ such that for all $x\in\mathbb{R}$ with $|x|\ge B_\delta$ one has

$$(1-\delta)|c_f||x|^n\le|f(x)|\le(1+\delta)|c_f||x|^n.$$

It follows that for any $\delta\in(0,1/2)$ one has

$$\begin{aligned}\liminf_{B\to\infty}\frac{U_\delta(f,\Sigma,\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}(\log B)^{s-1}} &\le \liminf_{B\to\infty}\frac{U(f,\Sigma,\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}(\log B)^{s-1}}\\ &\le \liminf_{B\to\infty}\frac{U_{-\delta}(f,\Sigma,\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}(\log B)^{s-1}}\end{aligned}$$

and

$$\limsup_{B\to\infty} \frac{U_\delta(f,\Sigma,\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}(\log B)^{s-1}} \leq \limsup_{B\to\infty} \frac{U(f,\Sigma,\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}(\log B)^{s'-1}} \leq \limsup_{B\to\infty} \frac{U_{-\delta}(f,\Sigma,\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}(\log B)^{s-1}},$$

where

$$U_{\pm\delta}(f,\Sigma,\varepsilon,B,\gamma,\sigma) := \sum_{h\in\mathbb{N}_S} 2\min\left\{B, ((1\pm\delta)^{-\varepsilon}|c_f|^{-\varepsilon}\gamma h)^{1/(n\varepsilon)}\right\}\cdot h^\sigma.$$

On the other hand, one has

$$\liminf_{B\to\infty} \frac{U_{\pm\delta}(f,\{q\},\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}} = 2\cdot\lambda^-(n,\sigma,q,\varepsilon)\cdot(1\pm\delta)^{-\sigma\varepsilon}|c_f|^{\sigma\varepsilon}\gamma^{-\sigma},$$
$$\limsup_{B\to\infty} \frac{U_{\pm\delta}(f,\{q\},\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}} = 2\cdot\lambda^+(n,\sigma,q,\varepsilon)\cdot(1\pm\delta)^{-\sigma\varepsilon}|c_f|^{\sigma\varepsilon}\gamma^{-\sigma},$$

by theorem 2.0.2, and

$$\lim_{B\to\infty} \frac{U_{\pm\delta}(f,\Sigma,\varepsilon,B,\gamma,\sigma)}{B^{1+\sigma n\varepsilon}(\log B)^{s-1}} = 2\cdot c(\Sigma)\cdot\frac{(1\pm\delta)^{-\varepsilon}|c_f|^{\sigma\varepsilon}\gamma^{-\sigma}}{-\sigma(1+\sigma n\varepsilon)}$$

when $s\geq 2$, by theorem 2.0.3.

Both claims (a) and (b) in the proposition follow now by taking the limit $\delta\to 0^+$. □

For the next definition we recall that a form $F\in\mathbb{Z}[X_1,\ldots,X_m]$ is said to be *of finite type* if

$$\mathrm{vol}(F) := \mu_\infty^m(\{\mathbf{x}\in\mathbb{R}^m : |F(\mathbf{x})|\leq 1\}) < \infty. \tag{2.21}$$

Definition 2.5.4. *Let $F\in\mathbb{Z}[X_1,\ldots,X_m]$ $(m\geq 2)$ be a form of finite type, $B,\gamma,\varepsilon\in\mathbb{R}_{>0}$, $\sigma\in\mathbb{R}_{<0}$, $\nu_1,\ldots,\nu_s\in\mathbb{Z}_{\geq 1}$ and let $\Sigma=\{q_1,\ldots,q_s\}$ be a multiplicative independent subset of $\mathbb{R}_{>1}$. We define*

$$U(F,\Sigma,\varepsilon,B,\gamma,\sigma,\nu_1,\ldots,\nu_s) := \sum_{h\in\mathbb{N}_\Sigma} \mu_\infty^m(V_F(B,(\gamma h)^{1/\varepsilon}))\left(\prod_{i=1}^s v_{q_i}(h)^{\nu_i-1}\right)\cdot h^\sigma.$$

Proposition 2.5.5. *In the above setting, suppose* $\varepsilon \in \left(0, -\frac{1}{\sigma n}\right)$. *Then*

$$U(F,\Sigma,\varepsilon,B,\gamma,\sigma,\nu_1,\dots,\nu_s) \asymp B^{m+\sigma n\varepsilon}(\log B)^{\nu_1+\dots+\nu_s-1} \quad \textit{as } B \to \infty.$$

Proof. Because of homogeneity we have

$$\mu_\infty^m(\{\mathbf{x} \in \mathbb{R}^m \ : \ |F(\mathbf{x})| \le M\}) = \mathrm{vol}(F) \cdot M^{m/n}, \quad \forall M \in \mathbb{R}_{>0},$$

which implies

$$\mu_\infty^m(V_F(B,M)) \le \min\{(2B)^m, \mathrm{vol}(F) \cdot M^{m/n}\} \quad \forall B, M \in \mathbb{R}_{>0}.$$

It follows that

$$\begin{aligned} &U(F,\Sigma,\varepsilon,B,\gamma,\sigma,\nu_1,\dots,\nu_s) \\ &\qquad \le \sum_{h \in \mathbb{N}_\Sigma} \min\{(2B)^m, \mathrm{vol}(F)\cdot(\gamma h)^{m/(n\varepsilon)}\}\left(\prod_{i=1}^s v_{q_i}(h)^{\nu_i-1}\right)\cdot h^\sigma \\ &\qquad \ll B^{m+\sigma n\varepsilon}(\log B)^{\nu_1+\dots+\nu_s-1} \quad \text{as } B \to \infty \end{aligned}$$

by proposition (2.4.5(a)).

On the other hand, letting

$$C_F := \max_{\|\mathbf{x}\|=1} F(\mathbf{x}),$$

we see that

$$\mu_\infty^m(V_F(B,M)) = (2B)^m \quad \forall M > C_F B^n$$

and thus

$$\begin{aligned} &U(F,\Sigma,\varepsilon,B,\gamma,\sigma,\nu_1,\dots,\nu_s) \\ &\qquad \ge \sum_{\substack{h \in \mathbb{N}_\Sigma \\ h > \gamma^{-1}(C_F B^n)^\varepsilon}} \mu_\infty(V_F(B,(\gamma h)^{1/\varepsilon}))\left(\prod_{i=1}^s v_{q_i}(h)^{\nu_i-1}\right)\cdot h^\sigma \\ &\qquad = (2B)^m \sum_{\substack{h \in \mathbb{N}_\Sigma \\ h > \gamma^{-1}(C_F B^n)^\varepsilon}} v_{p_1}(h)^{\nu_1-1}\dots v_{p_s}(h)^{\nu_s-1}h^\sigma \\ &\qquad \gg B^{m+\sigma n\varepsilon}(\log B)^{\nu_1+\dots+\nu_s-1} \quad \text{as } B \to \infty \end{aligned}$$

by proposition (2.4.5(b)). □

Chapter 3

Univariate polynomials

Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 1$, S a finite set of primes, $\varepsilon \in \left(0, \frac{1}{n}\right)$, $\gamma, B \in \mathbb{R}_{>0}$.

In this chapter, we study the asymptotic behaviour of the quantity

$$N(f, S, \varepsilon, B, \gamma) := \#\{x \in \mathbb{Z} : |x| \leq B,\, 0 < |f(x)|^{\varepsilon} \leq \gamma \cdot [f(x)]_S\} \tag{3.1}$$

as $B \to \infty$.

3.1 Translation into the adelic setting

Adjusting an idea from [Liu15, chapter 1], we interpret the set

$$\{x \in \mathbb{Z} : |x| \leq B,\, 0 < |f(x)|^{\varepsilon} \leq \gamma \cdot [f(x)]_S\} \tag{3.2}$$

as the set of integer point in the adelic region

$$\mathbb{A}(f, S, \varepsilon, B, \gamma) := \left\{ (x_v)_v \in \mathbb{A} \,:\, \begin{array}{c} |x_\infty| \leq B,\; |x_v|_v \leq 1 \,\forall v \neq \infty \\ 0 < |f(x_\infty)|^{\varepsilon} \prod_{p \in S} |f(x_p)|_p \leq \gamma \end{array} \right\}, \tag{3.3}$$

and we approximate (3.1) with the normalized Haar measure of (3.3) as $B \to \infty$.

An upper bound on the asymptotic rate of the difference

$$\left|\#(\mathbb{Z} \cap \mathbb{A}(f, S, \varepsilon, B, \gamma)) - \mu(\mathbb{A}(f, S, \varepsilon, B, \gamma))\right| \tag{3.4}$$

as $B \to \infty$ by a power of $\log B$ can be given in a similar fashion to the proof of [Liu15, Proposition 1.4.6].

Lemma 3.1.1. *Let $f(X) \in \mathbb{R}[X]$. For any $a \in \mathbb{R}$ and $\lambda, B, M \in \mathbb{R}_{>0}$ one has*

$$\left| \#((a + \lambda \mathbb{Z}) \cap V_f(B, M)) - \frac{\mu_\infty(V_f(B, M))}{\lambda} \right| \leq 2(n+1).$$

Proof. Note that the set $V_f(B, M)$ can be written as a disjoint union of $N \leq n+1$ intervals, say

$$V_f(B, M) = \bigcup_{j=1}^{N} I_j,$$

from which it follows that

$$\begin{aligned}
&\left| \#((a + \lambda \mathbb{Z}) \cap V_f(B, M)) - \frac{\mu_\infty(V_f(B, M))}{\lambda} \right| \\
&\qquad \leq \sum_{j=1}^{N} \left| \#((a + \lambda \mathbb{Z}) \cap I_j) - \frac{\mu_\infty(I_j)}{\lambda} \right| \\
&\qquad = \sum_{j=1}^{N} \left| \#\Big(\mathbb{Z} \cap \Big(-\frac{a}{\lambda} + \frac{1}{\lambda} I_j \Big) \Big) - \mu_\infty\Big(-\frac{a}{\lambda} + \frac{1}{\lambda} I_j \Big) \right| \\
&\qquad \leq 2N \\
&\qquad \leq 2(n+1)
\end{aligned}$$

□

The desired upper bound on the rate of (3.4) as $B \to \infty$ reads as follows.

Proposition 3.1.2. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 1$ and splitting field K over $\mathbb{Q}$, and denote by n_0 the number of distinct roots of f in K. Let S be a finite set of primes, with $s := \#S > 0$. Then for any $\varepsilon \in \left(0, \frac{1}{n}\right)$ and $\gamma \in \mathbb{R}_{>0}$ one has*

$$\left| \#(\mathbb{Z} \cap \mathbb{A}(f, S, \varepsilon, B, \gamma)) - \mu(\mathbb{A}(f, S, \varepsilon, B, \gamma)) \right| \ll_{f,S} (\log B)^{n_0 s} \quad \text{as } B \to \infty,$$

with implied constant independent of γ and ε.

Proof. Let us first fix once an for all a numbering for the roots $\alpha_1, \ldots, \alpha_n$ the root of f in K. This defines an equivalence relation on $\{1, \ldots, n\}$, namely

$$\forall i, j \in \{1, \ldots, n\}, \quad i \sim j \overset{\text{def}}{\iff} \alpha_i = \alpha_j. \tag{3.5}$$

Let

$$\{1,\dots,n\} = \mathcal{A}_1 \cup \dots \cup \mathcal{A}_{n_0},$$

be the equivalence class decomposition for the equivalence relation (3.5). We have then the factorization

$$f(X) = c_f\,(X-\alpha_1)\dots(X-\alpha_n) = c_f \prod_{i=1}^{n_0}\prod_{\alpha\in\mathcal{A}_i}(X-\alpha)$$

in $K[X]$, for some $c_f \in \mathbb{Z}_{\neq 0}$ (leading coefficient of f).

Now, let $p \in S$ and let $\mathfrak{p}$ be a prime of K above p. Since K is Galois over $\mathbb{Q}$, the ramification index $e(\mathfrak{p}/p)$ does not depend on the particular choice of $\mathfrak{p}$, so we can denote it by e_p without creating any confusion. We also denote by α_{pj} the image of α_j under the embedding $K \hookrightarrow K_{\mathfrak{p}}$ for any $j \in \{1,\dots,n\}$.

We denote

$$\mathcal{J}_0 := \{(p,j)\ :\ p\in S,\ j\in\{1,\dots,n\}\}$$

and we write the set $\mathbb{A}(f,S,\varepsilon,B,\gamma)$ as a disjoint union

$$\mathbb{A}(f,S,\varepsilon,B,\gamma) = \bigcup_{\mathbf{k}\in\mathcal{K}(B)} \mathbb{V}(\mathbf{k};B),$$

where we define

$$\mathbb{V}(\mathbf{k};B) := \left\{ (x_v)_v \in \mathbb{A}(f,S,\varepsilon,B,\gamma)\ :\ \begin{array}{c} |x_p-\alpha_{pj}|_p = p^{-k_{pj}/e_p} \\ \forall (p,j)\in\mathcal{J}_0 \end{array} \right\}$$

for any $\mathbf{k} \in \mathbb{Z}^{\mathcal{J}_0}$ and we denote

$$\mathcal{K}(B) := \{\mathbf{k}\in\mathbb{Z}^{\mathcal{J}_0}\ :\ \mathbb{V}(\mathbf{k};B)\neq\emptyset\}.$$

Note that, if $\mathbf{k}\in\mathcal{K}(B)$ and $(x_v)_v \in \mathbb{V}(\mathbf{k};B)$, then one has

$$\begin{aligned} p^{-k_{pj}/e_p} &\le \max\left\{|x_p|_p, |\alpha_{pj}|_p\right\} \\ &\le \max\left\{1, \max_{j\in\{1,\dots,n\}} |\alpha_{pj}|_p\right\} \quad \forall (p,j)\in\mathcal{J}_0 \end{aligned}$$

and thus

$$k_{pj} \geq -d_p \quad \forall (p,j) \in \mathcal{J}_0,$$

where

$$d_p := e_p \cdot \log_p \left(\max \left\{ 1, \max_{j \in \{1,\ldots,n\}} |\alpha_{pj}|_p \right\} \right) \in \mathbb{Z}_{\geq 0}\,.$$

It follows that

$$\mathcal{K}(B) \subseteq \mathcal{H} := \left\{ \mathbf{k} \in \mathbb{Z}^{\mathcal{J}_0} : \begin{array}{c} k_{pj} \geq -d_p \ \forall j \in \{1,\ldots,n\}, \\ k_{pi} = k_{pj} \quad \text{if } i \sim j \end{array} \right\}$$

for all $B \in \mathbb{R}_{>0}$ and thus

$$\begin{aligned} &\#\Big\{ \mathbf{k} \in \mathcal{K}(B) \,:\, \prod_{(p,j)\in\mathcal{J}_0} p^{k_{pj}/e_p} = h \Big\} \\ &\qquad \leq \#\Big\{ \mathbf{k} \in \mathcal{H} \,:\, \sum_{j=1}^{n} k_{pj} = v_{p^{1/e_p}}(h) \ \forall p \in S \Big\} \end{aligned} \tag{3.6}$$

for all $B \in \mathbb{R}_{>0}$ and $h \in \mathbb{N}_\Sigma$, where

$$\Sigma := \{ p^{1/e_p} \,:\, p \in S \}.$$

One can show, with an elementary combinatorial argument, that there exists a constant $C \in \mathbb{R}_{\geq 0}$ (independent of B) such that for all $h \in \mathbb{N}_\Sigma$ with $v_q(h) \geq 1\ \forall q \in \Sigma$ the quantity on the right-hand side of (3.6) is less or equal than

$$C \cdot \prod_{q \in \Sigma} v_q(h)^{n_0 - 1}.$$

Now, using the obvious inequality

$$\mu(\mathbb{V}(\mathbf{k}; B)) \leq 2B \cdot \Big(\prod_{(p,j)\in\mathcal{J}} p^{-k_{pj}/e_p} \Big)^{1/n}$$

and the fact that, for B big enough (depending on $f, S, \varepsilon, \gamma$), one has

$$\mathbb{Z} \cap \mathbb{V}(\mathbf{k}; B) = \emptyset \quad \forall \mathbf{k} \in \mathcal{K}(B) \setminus \mathcal{K}'(B),$$

where

$$\mathcal{K}'(B) := \Big\{ \mathbf{k} \in \mathcal{K}(B) \ : \ \sum_{(p,j)\in\mathcal{J}_0} \frac{k_{pj}}{e_p} \leq 2n \cdot \log B \Big\},$$

we deduce from proposition 2.4.5 that, for B big enough (depending on $f, S, \varepsilon, \gamma$), one has

$$\begin{aligned}
\sum_{\mathbf{k}\in\mathcal{K}(B)\setminus\mathcal{K}'(B)} & \big|\#(\mathbb{Z}\cap\mathbb{V}(\mathbf{k};B)) - \mu(\mathbb{V}(\mathbf{k};B))\big| \\
&= \sum_{\mathbf{k}\in\mathcal{K}(B)\setminus\mathcal{K}'(B)} \mu(\mathbb{V}(\mathbf{k};B)) \\
&\leq \sum_{\substack{h\in\mathbb{N}_\Sigma \\ h>B^{2n}}} \sum_{\substack{\mathbf{k}\in\mathcal{K}(B) \\ \prod_{(p,j)\in\mathcal{J}_0} p^{k_{pj}/e_p}=h}} \mu(\mathbb{V}(\mathbf{k};B)) \\
&\ll_{f,S} B \cdot \sum_{\Sigma'\subseteq\Sigma} \sum_{\substack{h\in\mathbb{N}_{\Sigma\setminus\Sigma'} \\ v_q(h)\geq 1\,\forall q\in\Sigma' \\ h>B^{2n}}} \Big(\prod_{q\in\Sigma'} v_q(h)^{n_0-1}\Big) h^{-1/n} \\
&\ll_{f,S} B^{-1}(\log B)^{n_0 s-1} \quad \text{as } B\to\infty,
\end{aligned}$$

with implied constants independent of γ and ε.

This proves that

$$\begin{aligned}
\sum_{\mathbf{k}\in\mathcal{K}(B)} & \big|\#(\mathbb{Z}\cap\mathbb{V}(\mathbf{k};B)) - \mu(\mathbb{V}(\mathbf{k};B))\big| \\
&= \sum_{\mathbf{k}\in\mathcal{K}'(B)} \big|\#(\mathbb{Z}\cap\mathbb{V}(\mathbf{k};B)) - \mu(\mathbb{V}(\mathbf{k};B))\big| + \mathcal{O}_{f,S}(B^{-1}(\log B)^{n_0 s-1})
\end{aligned} \tag{3.7}$$

as $B\to\infty$.

Let $\mathbf{k}\in\mathcal{K}'(B)$. For each subset $\mathcal{J}\subseteq\mathcal{J}_0$, we consider the subset $\mathbb{V}(\mathbf{k},\mathcal{J};B)$ of $\mathbb{V}(\mathbf{k};B)$ defined by the inequalities

$$\begin{cases} |x_p-\alpha_{pj}|_p < p^{-k_{pj}/e_p} & \forall (p,j)\in\mathcal{J}, \\ |x_p-\alpha_{pj}|_p \leq p^{-k_{pj}/e_p} & \forall (p,j)\in\mathcal{J}_0\setminus\mathcal{J}. \end{cases}$$

Since

$$\mathbb{V}(\mathbf{k};B) = \mathbb{V}(\mathbf{k},\emptyset;B) \setminus \bigcap_{\substack{\mathcal{J}\subseteq\mathcal{J}_0 \\ \#\mathcal{J}=1}} \mathbb{V}(\mathbf{k},\mathcal{J};B),$$

the inclusion-exclusion principle yields

$$\mu(\mathbb{V}(\mathbf{k};B)) = \sum_{l=0}^{ns}(-1)^l \sum_{\substack{\mathcal{J}\subseteq\mathcal{J}_0 \\ \#\mathcal{J}=l}} \mu(\mathbb{V}(\mathbf{k},\mathcal{J};B)) \tag{3.8}$$

and

$$\#(\mathbb{Z}\cap\mathbb{V}(\mathbf{k};B)) = \sum_{l=0}^{ns}(-1)^l \sum_{\substack{\mathcal{J}\subseteq\mathcal{J}_0 \\ \#\mathcal{J}=l}} \#(\mathbb{Z}\cap\mathbb{V}(\mathbf{k},\mathcal{J};B)). \tag{3.9}$$

If $\mathbb{V}(\mathbf{k},\mathcal{J};B) = \emptyset$, then clearly $\#(\mathbb{Z}\cap\mathbb{V}(\mathbf{k},\mathcal{J};B)) = \mu(\mathbb{V}(\mathbf{k},\mathcal{J};B)) = 0$. If on the contrary the set $\mathbb{V}(\mathbf{k},\mathcal{J};B)$ is non-empty, then it is of the form

$$V_f(B,M) \times \prod_{p\in S}(\alpha_p + p^{\kappa_p}\mathbb{Z}_p)$$

for some $M \in \mathbb{R}_{>0}$, $\kappa_p \in \mathbb{Z}_{\geq 0}$, $\alpha_p \in \{0,\dots,p^{\kappa_p}-1\}$ $(p \in S)$, with

$$\kappa_p \geq \max_{j\in\{1,\dots,n\}} \frac{k_{pj}}{e_p}.$$

Combined with the Chinese remainder theorem, this implies that, letting

$$h_0 := \prod_{p\in S} p^{\kappa_p},$$

one has[1]

$$\mathbb{Z}\cap\mathbb{V}(\mathbf{k},\mathcal{J};B) = (\alpha + h_0\mathbb{Z}) \cap V_f(B,M) \tag{3.10}$$

for some $\alpha \in \{0,\dots,h-1\}$. From lemma 3.1.1, it follows then that

$$\left|\#(\mathbb{Z}\cap\mathbb{V}(\mathbf{k},\mathcal{J};B)) - \mu(\mathbb{V}(\mathbf{k},\mathcal{J};B))\right| \leq 2(n+1) \quad \forall\mathbf{k}\in\mathcal{K}(B),\ \mathcal{J}\subseteq\mathcal{J}_0, \tag{3.11}$$

Combining (3.11) with (3.8) and (3.9), we get

$$\left|\#(\mathbb{Z}\cap\mathbb{V}(\mathbf{k};B)) - \mu(\mathbb{V}(\mathbf{k};B))\right| \leq 2^{ns+1}(n+1) \quad \forall\mathbf{k}\in\mathcal{K}(B). \tag{3.12}$$

[1]Even if we do not use a different notation (in order not to make it too heavy), it is important to understand that in (3.10) the intersection symbols on the left- and right-hand side have different meanings. On the left-hand side, $\mathbb{Z}$ is embedded diagonally into $\mathbb{A}$ and the set-theoretic intersection is taken in the universe $\mathbb{A}$. On the right-hand side, $\mathbb{Z}$ is embedded into $\mathbb{R}$ via the usual inclusion and the set-theoretic intersection is taken in the universe $\mathbb{R}$ (embedded diagonally in $\mathbb{A}$).

Now, an elementary combinatorial computation shows that

$$\#\mathcal{K}'(B) \ll_{f,S} (\log B)^{n_0 s} \quad \text{as } B \to \infty,$$

which, combined with (3.12), implies

$$\begin{aligned} \sum_{\mathbf{k}\in\mathcal{K}'(B)} &\left| \mathbb{Z} \cap \mathbb{A}(f,S,\varepsilon,B,\gamma) - \mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) \right| \\ &\ll_{f,S} (\log B)^{n_0 s} \quad \text{as } B \to \infty, \end{aligned} \tag{3.13}$$

with implied constant independent of γ and ε.

From (3.7) and (3.13), we deduce that

$$\begin{aligned} &\left|\#(\mathbb{Z}\cap\mathbb{A}(f,S,\varepsilon,B,\gamma)) - \mu(\mathbb{A}(f,S,\varepsilon,B,\gamma))\right| \\ &\qquad \le \sum_{\mathbf{k}\in\mathcal{K}(B)} \left|\#(\mathbb{Z}\cap\mathbb{A}(f,S,\varepsilon,B,\gamma)) - \mu(\mathbb{A}(f,S,\varepsilon,B,\gamma))\right| \\ &\qquad \ll_{f,S} (\log B)^{n_0 s} \quad \text{as } B \to \infty, \end{aligned}$$

with implied constant independent of γ and ε, which is what we wanted to prove. □

3.2 Asymptotic behaviour of the (candidate) main term

Needless to say, proposition 3.1.2 says something interesting about the asymptotic behaviour of $N(f,S,\varepsilon,B,\gamma)$ as $B \to \infty$ only if one can also prove that $\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma))$ grows faster that the upper bound on the rate of the (candidate) error term (3.4) as $B \to \infty$.

In this section, we prove general results on the asymptotic behaviour of $N(f,S,\varepsilon,B,\gamma)$ as $B \to \infty$ by combining proposition 3.1.2 with the study of the asymptotic behaviour of the (candidate) main term $\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma))$ as $B \to \infty$.

Let us start by writing $\mathbb{A}(f,S,\varepsilon,B,\gamma)$ as a disjoint union

$$\mathbb{A}(f,S,\varepsilon,B,\gamma) = \bigcup_{h\in\mathbb{N}_S} \mathbb{A}_h(f,S,\varepsilon,B,\gamma), \tag{3.14}$$

where for any $h \in \mathbb{N}_S$ we denote

$$\mathbb{A}_h(f,S,\varepsilon,B,\gamma) := \Big\{(x_v)_v \in \mathbb{A}(f,S,\varepsilon,B,\gamma) \;:\; \prod_{p\in S} |f(x_p)|_p = h^{-1}\Big\}. \tag{3.15}$$

If $h = \prod_{p\in S} p^{k_p}$, then it follows immediately from (3.15) that

$$\begin{aligned}\mu(\,&\mathbb{A}_h(f,S,\varepsilon,B,\gamma)) \\ &= \mu_\infty(V_f(B,(\gamma h)^{1/\varepsilon}))\prod_{p\in S}\mu_p(\{x\in\mathbb{Z}_p \;:\; |f(x)|_p = p^{-k_p}\}).\end{aligned} \tag{3.16}$$

Let $S' \subseteq S$ be the subset of all $p \in S$ such that $Z_{f,p}(T) \notin \mathbb{Z}_{(p)}[T]$ (equivalently, f has a root in $\mathbb{Z}_p$). For each $p \in S \setminus S'$, we denote by $u_p(f)$ the largest positive integer u such that $\mu_p(\{x\in\mathbb{Z}_p : |f(x)|_p = p^{-u}\}) > 0$.

Defining

$$H_0 := \prod_{p\in S\setminus S'} p^{u_p(f)}, \qquad C_{h_0}(f) := \sum_{h_0'|H_0h_0^{-1}} \mu(h_0')\frac{N_{h_0h_0'}(f)}{h_0h_0'} \quad (h_0|H_0), \tag{3.17}$$

it follows from (3.14) that

$$\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) = \sum_{h_0|H_0} C_{h_0}(f)\cdot\mu(\mathbb{A}(f,S',\varepsilon,B,\gamma h_0)). \tag{3.18}$$

From corollary 1.1.6, lemma 1.2.5 and proposition 2.5.3, we deduce the following result.

Theorem 3.2.1. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 1$ and leading coefficient c_f. Denote by $R(f)$ maximum multiplicity of a root of f. Let S be a finite set of primes and let $S' \subseteq S$ be the subset of all $p \in S$ such that f has a root in $\mathbb{Z}_p$. Suppose that $s' := \#S' > 0$. Then for all $\varepsilon \in \left(0,\frac{1}{n}\right)$ one has*

$$N(f,S,\varepsilon,B,\gamma) \asymp_{f,S} \frac{|c_f|^{-\varepsilon/R(f)}\gamma^{1/R(f)}}{R(f)-n\varepsilon}\cdot B^{1-(n\varepsilon)/R(f)}(\log B)^{s'-1} \quad \text{as } B\to\infty,$$

with implied constants independent of γ and ε.

Proof. In light of proposition 3.1.2, it is enough to prove that

$$\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) \asymp_{f,S} \frac{|c_f|^{-\varepsilon/R(f)}\gamma^{1/R(f)}}{R(f)-n\varepsilon} \cdot B^{1-(n\varepsilon)/R(f)}(\log B)^{s'-1} \tag{3.19}$$

Because of (3.18), we may assume without loss of generality that $S = S'$. From corollary 1.1.6 and proposition 1.2.7, it follows that there exist $C \in \mathbb{R}_{>1}$ (independent of ε and γ) and $a_p, N_p \in \mathbb{Z}_{\geq 1}$ (dependent only on f and p) for each $p \in S$, such that, for any $h = \prod_{p\in S} p^{k_p} \in \mathbb{N}_S$, one has

$$\begin{aligned}\mu(\mathbb{A}_h(f,S,\varepsilon,B,\gamma)) &= \mu_\infty(V_f(B,(\gamma h)^{1/\varepsilon}))\prod_{p\in S}\mu_p(\{\mathbf{x}\in\mathbb{Z}_p^m : |f(\mathbf{x})|_p = p^{-k_p}\})\\ &\leq C\cdot\mu_\infty(V_f(B,(\gamma h)^{1/\varepsilon}))\cdot h^{-1/R(f)}\end{aligned}$$

and for any $\widetilde{h} = \prod_{p\in S} p^{N_p\widetilde{k}_p} \in \mathbb{N}_{\widetilde{S}}$ one has

$$\begin{aligned}&\mu(\mathbb{A}_{h^*\widetilde{h}}(f,S,\varepsilon,B,\gamma))\\ &\quad= \mu_\infty(V_f(B,(\gamma h^*\widetilde{h})^{1/\varepsilon}))\prod_{p\in S}\mu_p(\{\mathbf{x}\in\mathbb{Z}_p^m : |f(\mathbf{x})|_p = p^{a_p+N_p\widetilde{k}_p}\})\\ &\quad\geq \frac{1}{C}\cdot\mu_\infty(V_f(B,(\gamma\widetilde{h})^{1/\varepsilon}))\cdot(\widetilde{h})^{-1/R(f)},\end{aligned}$$

where we denote

$$h^* := \prod_{p\in S} p^{a_p}, \qquad \widetilde{S} := \{p^{N_p} : p \in S\}.$$

In the notation from chapter 2, this proves that

$$\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) \leq C\cdot U\big(f,S,\varepsilon,B,\gamma,-1/R(f)\big) \tag{3.20}$$

and

$$\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) \geq \frac{1}{C}\cdot U\big(f,\widetilde{S},\varepsilon,B,\gamma,-1/R(f)\big) \tag{3.21}$$

The claim (3.19) follows now from (3.20), (3.21) and proposition 2.5.3. □

Remark 3.2.2. *If $S' = \emptyset$, then $N(f,S,\varepsilon,B,\gamma)$ is eventually constant as $B \to \infty$.*

3.3 The non-zero discriminant case

Theorem 3.2.1 generalizes [BEG18, Theorem 2.3] to univariate polynomials of possibly zero discriminant. Indeed, if $f \in \mathbb{Z}[X]$ has discriminant $\Delta \neq 0$, then $R(f) = 1$. Moreover, the definition of S' agrees with the one given in [BEG18, Theorem 2.3] under the assumption of that theorem. This follows from a result of Stewart ([Ste91]), according to which for a polynomial $f \in \mathbb{Z}[X]$ of degree $n \geq 2$ and discriminant $\Delta \neq 0$ one has

$$N_{p^k}(f) = N_{p^{v_p(\Delta)+1}}(f) \quad \forall k \geq v_p(\Delta) + 1. \tag{3.22}$$

If

$$x \equiv a_j \mod p^k \quad (j = 1, \dots, N_{p^k}(f)) \tag{3.23}$$

is the complete solution of the congruence $f(x) \equiv 0 \mod p^k$, then

$$\mu_p(\{x \in \mathbb{Z}_p : |f(x)|_p \leq p^{-k}\}) = \sum_{j=1}^{N_{p^k}(f)} \mu_p(a_j + p^k \mathbb{Z}_p) = \frac{N_{p^k}(f)}{p^k} \tag{3.24}$$

and thus

$$\begin{aligned} \mu_p(\{x \in \mathbb{Z}_p : &|f(x)|_p = p^{-k}\}) \\ &= \frac{pN_{p^k}(f) - N_{p^{k+1}}(f)}{p^{k+1}} \\ &= \left(1 - \frac{1}{p}\right) N_{p^{v_p(\Delta)+1}}(f) \cdot p^{-k} \quad \forall k \geq v_p(\Delta) + 1, \end{aligned} \tag{3.25}$$

which shows that

$$Z_{f,p}(T) = P(T) + \frac{\left(1 - \frac{1}{p}\right) N_{p^{v_p(\Delta)+1}}(f)}{1 - p^{-1}T}, \tag{3.26}$$

for some polynomial $P \in \mathbb{Z}_{(p)}[T]$ of degree less or equal to $v_p(\Delta)$, from which the equivalence of the two definitions for S' is clear.

In this section we explain how to combine (3.22) with proposition 2.5.3 in order to improve the asymptotics given in [BEG18, Theorem 2.3].

In what follows we denote

$$H := \prod_{p\in S'} p^{v_p(\Delta)+1}. \tag{3.27}$$

Lemma 3.3.1. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ and discriminant $\Delta \neq 0$. Let S be a finite set of primes with $s := \#S \geq 2$ and such that the congruence $f(x) \equiv 0 \mod p^{v_p(\Delta)+1}$ is solvable for all $p \in S$. Then for any $\varepsilon \in \left(0, \frac{1}{n}\right)$ one has*

$$\left|\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) - \left(\prod_{p\in S}\left(1-\frac{1}{p}\right)\right)\frac{N_H(f)}{H}\cdot U(f,S,\varepsilon,B,\gamma H,-1)\right|$$
$$\ll_{f,S,\varepsilon} \gamma\cdot B^{1-n\varepsilon}(\log B)^{s-2} \quad \text{as } B\to\infty.$$

Proof. By (3.22) and the Chinese Remainder Theorem, one has

$$\begin{aligned}\prod_{p\in S}\mu_p(\{x\in\mathbb{Z}_p : |f(x)|_p = |Hh|_p\}) &= \sum_{h'\in\mathbb{N}_S}\mu(h')\frac{N_{Hhh'}(f)}{Hhh'}\\ &= \left(\prod_{p\in S}\left(1-\frac{1}{p}\right)\right)\frac{N_H(f)}{Hh}\end{aligned}$$

for all $h\in\mathbb{N}_S$.

Therefore

$$\begin{aligned}&\left|\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) - \left(\prod_{p\in S}\left(1-\frac{1}{p}\right)\right)\frac{N_H(f)}{H}\cdot U(f,S,\varepsilon,B,\gamma H,-1)\right|\\ &\quad= \left|\sum_{\substack{h\in\mathbb{N}_S\\ H\nmid h}}\left(\sum_{h'\in\mathbb{N}_S}\mu(h')\frac{N_{hh'}(f)}{h'}\right)\frac{\mu_\infty(V_f(B,(\gamma h)^{1/\varepsilon}))}{h}\right|\\ &\quad\leq \sum_{p\in S}\sum_{a=0}^{v_p(\Delta)+1}\frac{N_{p^a}(f)}{p^a}\sum_{h\in\mathbb{N}_{S\setminus\{p\}}}\frac{N_h(f)}{h}\cdot\mu_\infty(V_f(B,(\gamma h)^{1/\varepsilon}))\\ &\quad\ll_{f,S}\sum_{p\in S}U(f,S\setminus\{p\},\varepsilon,B,\gamma,-1)\\ &\quad\ll_{f,S,\varepsilon}\gamma\cdot B^{1-n\varepsilon}(\log B)^{s-2} \quad \text{as } B\to\infty.\end{aligned}$$

Note that we have used (3.22) and the Chinese Remainder Theorem again to get that $N_h(f) = \mathcal{O}_{f,S}(1)$. ☐

Theorem 3.3.2. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$, leading coefficient c_f and discriminant $\Delta \neq 0$. Let S be a finite set of primes and let S' denote the subset of all $p \in S$ such that the equation $f(x) \equiv 0 \mod p^{v_p(\Delta)+1}$ is solvable. Suppose that $s' := \#S' \geq 2$. Then one has*

$$N(f,S,\varepsilon,B,\gamma) \sim 2 \cdot \frac{C(f,S)N_H(f)}{1-n\varepsilon} \cdot \gamma\, |c_f|^{-\varepsilon} \cdot B^{1-n\varepsilon} (\log B)^{s'-1} \quad \textit{as } B \to \infty,$$

with

$$C(f,S) := \left(\sum_{h_0 | H_0} C_{h_0}(f) \right) \left(\prod_{p \in S'} \left(1 - \frac{1}{p}\right) \right) c(S'),$$

where $c(S')$ is the constant appearing in lemma 2.3.2.

Proof. Because of proposition 3.1.2, it suffices to prove that

$$\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) \sim 2 \cdot \frac{C(f,S)N_H(f)}{1-n\varepsilon} \cdot \gamma\, |c_f|^{-\varepsilon} \cdot B^{1-n\varepsilon} (\log B)^{s'-1} \tag{3.28}$$

as $B \to \infty$.

By (3.18) and lemma 3.3.1, we see that

$$\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma)) = 2 \cdot \frac{C(f,S)N_H(f)}{1-n\varepsilon} \cdot \gamma\, |c_f|^{-\varepsilon} \cdot \frac{1}{H} \cdot U(f,S,\varepsilon,B,\gamma H,-1) + \mathcal{O}_{f,S,\varepsilon,\gamma}(B^{1-n\varepsilon}(\log B)^{s-2}) \quad \text{as } B \to \infty.$$

The claim (3.28) follows then from proposition 2.5.3. □

If the set S' has only one element, then we do not have an exact asymptotics, i.e.

$$\frac{N(f,S,\varepsilon,B,\gamma)}{B^{1-n\varepsilon}} \tag{3.29}$$

does not admit a limit as $B \to \infty$.

In the case $S = S' = \{p\}$ we are even able to explicitly compute the exact lim inf and lim sup of the quantity (3.29) as $B \to \infty$.

Theorem 3.3.3. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$, leading coefficient c_f and discriminant $\Delta \neq 0$. Let S be a finite set of primes and let S' denote the subset of all $p \in S$ such that the equation $f(x) \equiv 0 \mod p^{v_p(\Delta)+1}$ is solvable. If $S' = \{p\}$, then*

$$\lim_{B\to\infty} \frac{N(f,S,\varepsilon,B,\gamma)}{B^{1-n\varepsilon}} \quad \textit{does } \underline{\textit{not}} \textit{ exist.}$$

In the case $S = S' = \{p\}$, we compute

$$\liminf_{B\to\infty} \frac{N(f,\{p\},\varepsilon,B,\gamma)}{B^{1-n\varepsilon}} = \lambda^-(n,-1,p,\varepsilon)\cdot|c_f|^{-\varepsilon}\gamma\cdot\frac{N_{p^{v_p(\Delta)+1}}}{p^{v_p(\Delta)+1}},$$
$$\limsup_{B\to\infty} \frac{N(f,\{p\},\varepsilon,B,\gamma)}{B^{1-n\varepsilon}} = \lambda^+(n,-1,p,\varepsilon)\cdot|c_f|^{-\varepsilon}\gamma\cdot\frac{N_{p^{v_p(\Delta)+1}}}{p^{v_p(\Delta)+1}},$$

where the quantities $\lambda^{\pm}(n,-1,p,\varepsilon)$ are as in definition 2.5.2.

Proof. Suppose $S' = \{p\}$. The fact that the quantity $\frac{\mu(\mathbb{A}(f,S,\varepsilon,B,\gamma))}{B^{1-n\varepsilon}}$ does not admit a limit as $B \to \infty$ (and so neither does $\frac{N(f,S,\varepsilon,B,\gamma)}{B^{1-n\varepsilon}}$ because of proposition 3.1.2) can be easily checked for example by taking the limits along the sequences $B_l = (|c_f|^{-\varepsilon}\gamma H p^l)^{1/(n\varepsilon)}$, $B'_l = (|c_f|^{-\varepsilon}\gamma H q p^l)^{1/(n\varepsilon)}$. A straightforward computation shows that both limits exist but they are different.

If $S = S' = \{p\}$, then we see that

$$\mu(\mathbb{A}(f,\{p\},\varepsilon,B,\gamma)) = \frac{1}{p^{v_p(\Delta)+1}}U(f,\{p\},\varepsilon,B,\gamma,-1) + \mathcal{O}_{f,p,\varepsilon,\gamma}(1) \qquad (3.30)$$

by (3.22).

From (3.30) and proposition 2.5.3, we get that

$$\liminf_{B\to\infty} \frac{\mu(\mathbb{A}(f,\{p\},\varepsilon,B,\gamma))}{B^{1-n\varepsilon}} = \lambda^-(n,-1,p,\varepsilon)\cdot|c_f|^{-\varepsilon}\gamma\cdot\frac{N_{p^{v_p(\Delta)+1}}(f)}{p^{v_p(\Delta)+1}},$$

and

$$\limsup_{B\to\infty} \frac{\mu(\mathbb{A}(f,\{p\},\varepsilon,B,\gamma))}{B^{1-n\varepsilon}} = \lambda^+(n,-1,p,\varepsilon)\cdot|c_f|^{-\varepsilon}\gamma\cdot\frac{N_{p^{v_p(\Delta)+1}}(f)}{p^{v_p(\Delta)+1}}.$$

The claims of the theorem follow now from 3.1.2. □

For the sake of completeness, we include the proof of a refinement of proposition 3.1.2 in the non-zero discriminant case.

Proposition 3.3.4. *Let $f \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$ and discriminant $\Delta \neq 0$. Let S be a finite set of primes and let S' denote the subset of all $p \in S$ such that the equation $f(x) \equiv 0 \mod p^{v_p(\Delta)+1}$ is solvable. Then one has*

$$\left|\#(\mathbb{Z} \cap \mathbb{A}(f,S,\varepsilon,B,\gamma)) - \mu(\mathbb{A}(f,S,\varepsilon,B,\gamma))\right| \ll_{f,S} (\log B)^{s'} \quad \textit{as } B \to \infty,$$

with implied constant independent of γ and ε.

Proof. For any $h, h' \in \mathbb{N}_S$ we denote

$$\widehat{N}_{h,h'}(f,S,\varepsilon,B,\gamma) := \#\{x \in \mathbb{Z} : |x| \leq B, |f(x)| \leq (\gamma h)^{1/\varepsilon}, f(x) \equiv 0 \mod hh'\}.$$

Let

$$x \equiv a_j \mod p^k \quad (j = 1, \dots, N_{p^k}(f))$$

be the solution of the congruence

$$f(x) \equiv 0 \mod p^k,$$

with $a_j \in \{0, \dots, p^k - 1\}$ for all j's. Lemma 3.1.1, together with the fact that $N_h(f) = \mathcal{O}_{f,S}(1)$, yields

$$\begin{aligned} \widehat{N}_h(f,S,\varepsilon,B,\gamma) &= \sum_{j=1}^{N_h(f)} \#((a_j + h\mathbb{Z}) \cap V_f(B,(\gamma h)^{1/\varepsilon})) \\ &= \frac{N_h(f)}{h} \mu_\infty(V_f(B,M)) + \mathcal{O}_{f,S}(1) \quad \text{as } B \to \infty, \end{aligned}$$

with implied constant independent of h.

The inclusion-exclusion principle, together with lemmas 3.1.1, gives us that

$$\begin{aligned}
\#(\mathbb{Z} \cap \mathbb{A}_h(f,S,\varepsilon,B,\gamma)) &= \sum_{h' \in \mathbb{N}_S} \mu(h') \widehat{N}_{h,h'}(f,S,\varepsilon,B,\gamma) \\
&= \Big(\sum_{h' \in \mathbb{N}_S} \mu(h') \frac{N_{hh'}(f)}{hh'} \Big) \mu_\infty(V_f(B,\gamma h^{1/\varepsilon})) + \mathcal{O}_{f,S}(1) \\
&= \mu_\infty(V_f(B,\gamma h^{1/\varepsilon})) \prod_{p \in S} \mu_p(\{x \in \mathbb{Z}_p \,:\, |f(x)|_p = p^{-v_p(h)}\}) + \mathcal{O}_{f,S}(1) \\
&= \mu(\mathbb{A}_h(f,S,\varepsilon,B,\gamma)) + \mathcal{O}_{f,S}(1) \quad \text{as } B \to \infty.
\end{aligned}$$

Now, let $C > 0$ be such that $|f(x)| \leq C(1+|x|)^n$ for any $x \in \mathbb{R}$. It follows that $\mathbb{Z} \cap \mathbb{A}_h(f,S,\varepsilon,B,\gamma) = \emptyset$ for any $h > C(1+B)^n$. Therefore

$$\begin{aligned}
&\Big| \#(\mathbb{Z} \cap \mathbb{A}(f,S,\varepsilon,B,\gamma)) - \sum_{\substack{h \in \mathbb{N}_S \\ h \leq C(1+B)^n}} \mu(\mathbb{A}_h(f,S,\varepsilon,B,\gamma)) \Big| \\
&\quad \leq \sum_{\substack{h \in \mathbb{N}_S \\ h \leq C(1+B)^n}} \big| \#(\mathbb{Z} \cap \mathbb{A}_h(f,S,\varepsilon,B,\gamma)) - \mu(\mathbb{A}_h(f,S,\varepsilon,B,\gamma)) \big| \\
&\quad = \sum_{h_0 | H} \sum_{\substack{h \in \mathbb{N}_{S'} \\ hh_0 \leq C(1+B)^n}} \big| \#(\mathbb{Z} \cap \mathbb{A}_{hh_0}(f,S,\varepsilon,B,\gamma)) - \mu(\mathbb{A}_{hh_0}(f,S,\varepsilon,B,\gamma)) \big| \\
&\quad \ll_{f,S} \sum_{h_0 | H} \#\{h \in \mathbb{N}_{S'} \,:\, hh_0 \leq C(1+B)^n\} \\
&\quad \ll_{f,S} (\log B)^{s'} \quad \text{as } B \to \infty.
\end{aligned}$$

The claim follows then by noticing that

$$\begin{aligned}
\sum_{\substack{h \in \mathbb{N}_S \\ h > C(1+B)^n}} \mu(\mathbb{A}_h(f,S,\varepsilon,B,\gamma)) &\ll_{f,S} \sum_{\substack{h \in \mathbb{N}_S \\ h > C(1+B)^n}} \frac{B}{h} \\
&\ll_{f,S} B^{1-n} (\log B)^{s'-1} \quad \text{as } B \to \infty.
\end{aligned}$$

□

Chapter 4

Decomposable forms of finite type

Let $F \in \mathbb{Z}[X_1, \ldots, X_m]$ be a decomposable form of degree $n > m$ and of finite type, S a finite set of primes, $\varepsilon \in \left(0, \frac{1}{n}\right)$, $\gamma, B \in \mathbb{R}_{>0}$.

In this chapter, we study the asymptotic behaviour of the quantity

$$N(F, S, \varepsilon, B, \gamma) := \#\{\mathbf{x} \in \mathbb{Z}^m_{\text{prim}} \,:\, \|\mathbf{x}\| \leq B,\, 0 < |F(\mathbf{x})|^\varepsilon \leq \gamma \cdot [F(\mathbf{x})]_S\} \quad (4.1)$$

as $B \to \infty$.

The reasonings in this context are very similar to the ones in the context of univariate polynomials in chapter 3. We interpret the set

$$\{\mathbf{x} \in \mathbb{Z}^m_{\text{prim}} \,:\, \|\mathbf{x}\| \leq B,\, 0 < |F(\mathbf{x})|^\varepsilon \leq \gamma \cdot [F(\mathbf{x})]_S\} \quad (4.2)$$

as the set of integer point in the adelic region

$$\mathbb{A}(F, S, \varepsilon, B, \gamma) := \left\{ (\mathbf{x}_v)_v \in \mathbb{A}^m \,:\, \begin{array}{c} \|\mathbf{x}_\infty\| \leq B,\, \|\mathbf{x}_v\|_v = 1 \,\forall v \neq \infty \\ 0 < |F(\mathbf{x}_\infty)|^\varepsilon \prod_{p \in S} |F(\mathbf{x}_p)|_p \leq \gamma \end{array} \right\}. \quad (4.3)$$

As in chapter 3, we give first an upper bound on the asymptotic rate of the (candidate) error term

$$\left|\#(\mathbb{Z}^m \cap \mathbb{A}(F, S, \varepsilon, B, \gamma)) - \mu^m(\mathbb{A}(F, S, \varepsilon, B, \gamma))\right| \quad (4.4)$$

as $B \to \infty$.

In this case, the desired upper bound follows from [Liu15, Proposition 1.4.6] by means an elementary computation.

Proposition 4.0.1. *Let $F \in \mathbb{Z}[X_1, \ldots, X_m]$ ($m \geq 2$) be a decomposable form of degree $n > m$ and of finite type. Let S be a finite set of primes, with $s := \#S \geq 1$. Then, for all $\varepsilon \in \left(0, \frac{1}{n}\right)$ and $\gamma \in \mathbb{R}_{>0}$, one has*

$$\left|\#(\mathbb{Z}^m \cap \mathbb{A}(F, S, \varepsilon, B, \gamma)) - \mu^m(\mathbb{A}(F, S, \varepsilon, B, \gamma))\right| \ll_{F,S,\varepsilon} B^{m-1}(\log B)^{ns+\delta}$$

as $B \to \infty$, with implied constant is independent of γ, where

$$\delta = \begin{cases} 1 & \text{if } m = 2, \\ 0 & \text{if } m \geq 3. \end{cases}$$

Proof. Let us first introduce the notation

$$\mathbb{A}^m_{S\cup\{\infty\}} := \mathbb{R}^m \times \prod_{p\in S} \mathbb{Z}^m_p, \qquad \mu^m_{S\cup\{\infty\}} := \bigotimes_{v\in S\cup\{\infty\}} \mu^m_v,$$

in accordance with the notation used in [Liu15]. We also denote

$$\mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B; \varepsilon) := \left\{ (\mathbf{x}_v)_v \in \mathbb{A}^m_{S\cup\infty} : \begin{array}{c} \|\mathbf{x}_\infty\| \leq B,\ \|\mathbf{x}_p\|_p = 1\,\forall p \in S, \\ 0 < |F(\mathbf{x}_\infty)|^\varepsilon \prod_{p\in S} |F(\mathbf{x}_p)|_p \leq \gamma \end{array} \right\} \tag{4.5}$$

and

$$\mathbb{E}(\gamma, B; \varepsilon) := \left|\#(\mathbb{Z}^m \cap \mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B; \varepsilon)) - \mu^m_{S\cup\{\infty\}}(\mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B; \varepsilon))\right|.$$

Note that $\mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B; 1)$ is the set denoted by $\mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B)$ in [Liu15]. Going through the proof of [Liu15, Proposition 1.4.6], one realizes that the whole argument would work exactly in the same way if one replaces $\mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B; 1)$ with $\mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B; \varepsilon)$ for any $\varepsilon \in \left(0, \frac{1}{n}\right)$.

The outcome is the upper bound

$$\mathbb{E}(\gamma, B; \varepsilon) \ll_{F,S,\varepsilon} B^{m-1}(\log B)^{ns} \quad \text{as } B \to \infty. \tag{4.6}$$

A straightforward application of the inclusion-exclusion principle gives us

$$\begin{aligned}
&\#(\mathbb{Z}^m \cap \mathbb{A}(F,S,\varepsilon,B,\gamma)) \\
&\quad = \#\{\mathbf{x} \in \mathbb{Z}^m \,:\, \|\mathbf{x}\| \le B,\ \|\mathbf{x}\|_p = 1\,\forall p \in S,\ 0 \le |F(\mathbf{x})|^\varepsilon \le \gamma \cdot [F(\mathbf{x})]_S\} \\
&\quad = \sum_{\substack{(d,p)=1\,\forall p\in S \\ d \le B}} \mu(d) \cdot \#\left\{\mathbf{y} \in \mathbb{Z}^m \,:\, \begin{array}{c} \|\mathbf{y}\| \le B/d,\ \|\mathbf{y}\|_p = 1\,\forall p \in S, \\ 0 \le d^{n\varepsilon}|F(\mathbf{y})|^\varepsilon \le \gamma \cdot [F(\mathbf{y})]_S \end{array}\right\} \\
&\quad = \sum_{\substack{(d,p)=1\,\forall p\in S \\ d \le B}} \mu(d) \cdot \#(\mathbb{Z}^m \cap \mathbb{A}_{F,S\cup\{\infty\}}(\gamma d^{-n\varepsilon}, B/d; \varepsilon))
\end{aligned}$$

and

$$\begin{aligned}
\mu^m(\mathbb{A}(F,S,\varepsilon,B,\gamma)) &= \left(\prod_{p \notin S}\left(1 - \frac{1}{p^m}\right)\right) \cdot \mu_{S\cup\{\infty\}}(\mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B; \varepsilon)) \\
&= \sum_{(d,p)=1\,\forall p\in S} \frac{\mu(d)}{d^m} \cdot \mu_{S\cup\{\infty\}}(\mathbb{A}_{F,S\cup\{\infty\}}(\gamma, B; \varepsilon)) \\
&= \sum_{(d,p)=1\,\forall p\in S} \mu(d) \cdot \mu_{S\cup\{\infty\}}(\mathbb{A}_{F,S\cup\{\infty\}}(\gamma d^{-n\varepsilon}, B/d; \varepsilon)).
\end{aligned}$$

Therefore, we get

$$\begin{aligned}
&\left|\#(\mathbb{Z}^m \cap \mathbb{A}(F,S,\varepsilon,B,\gamma)) - \mu^m(\mathbb{A}(F,S,\varepsilon,B,\gamma))\right| \\
&\qquad \le \sum_{(d,p)=1\,\forall p\in S} |\mu(d)| \cdot \mathbb{E}(\gamma d^{-n\varepsilon}, B/d; \varepsilon)
\end{aligned} \tag{4.7}$$

Now, if $m \ge 3$, then the combination of (4.6) and (4.7) yields

$$\begin{aligned}
&\left|\#(\mathbb{Z}^m \cap \mathbb{A}(F,S,\varepsilon,B,\gamma)) - \mu^m(\mathbb{A}(F,S,\varepsilon,B,\gamma))\right| \\
&\qquad \ll_{F,S,\varepsilon} \sum_{(d,p)=1\,\forall p\in S} |\mu(d)| \cdot \left(\frac{B}{d}\right)^{m-1}\left(\log\frac{B}{d}\right)^{ns} \\
&\qquad \le \zeta(m-1) \cdot B^{m-1}(\log B)^{ns} \quad \text{as } B \to \infty.
\end{aligned}$$

In the case $m = 2$, we see that instead

$$\begin{aligned}
\sum_{\substack{(d,p)=1\,\forall p\in S \\ d \le B}} |\mu(d)| \cdot \mathbb{E}(\gamma d^{-n\varepsilon}, B/d; \varepsilon) &\ll_{F,S,\varepsilon} \left(\sum_{d \le B} \frac{|\mu(d)|}{d}\right) \cdot B(\log B)^{ns} \\
&\ll_{F,S,\varepsilon} B(\log B)^{ns+1} \quad \text{as } B \to \infty
\end{aligned}$$

and

$$\begin{aligned}
\sum_{\substack{(d,p)=1\,\forall p\in S\\ d>B}} &|\mu(d)|\cdot\mu^2_{S\cup\{\infty\}}(\mathbb{A}_{F,S\cup\{\infty\}}(\gamma d^{-n\varepsilon},B/d;\varepsilon))\\
&=\Bigg(\sum_{\substack{(d,p)=1\,\forall p\in S\\ d>B}}\frac{|\mu(d)|}{d^2}\Bigg)\cdot\mu^2_{S\cup\{\infty\}}(\mathbb{A}_{F,S\cup\{\infty\}}(\gamma,B;\varepsilon))\\
&\leq B^2\cdot\sum_{d>B}\frac{|\mu(d)|}{d^2}\\
&\ll B \quad \text{as } B\to\infty.
\end{aligned}$$

It follows that

$$\sum_{(d,p)=1\,\forall p\in S}|\mu(d)|\cdot\mathbb{E}(\gamma d^{-n\varepsilon},B/d;\varepsilon)\ll_{F,S,\varepsilon} B(\log B)^{ns+1}\quad\text{as } B\to\infty$$

and thus

$$\begin{aligned}
&\big|\#(\mathbb{Z}^m\cap\mathbb{A}(F,S,\varepsilon,B,\gamma))-\mu^m(\mathbb{A}(F,S,\varepsilon,B,\gamma))\big|\\
&\qquad\qquad\ll_{F,S,\varepsilon} B(\log B)^{ns+1}\quad\text{as } B\to\infty.
\end{aligned}$$

by (4.7). □

Lemma 4.0.2. *If* $F\in\mathbb{Z}[X_1,\ldots,X_m]$ $(m\geq 2)$ *is a decomposable form of finite type, then* $\mathrm{rk}(F)=m$.

Proof. Suppose $rk(F)=t<m$ and let W be the maximal linear subspace of $\mathbb{R}^m$ at which all the linear factors of F vanish.

Replacing the linear factors of F by their real and imaginary parts, we get a new system of linear forms of the same rank and the same set of common zeros, so W has dimension $m-t$. It follows that there exist an orthogonal transformation $\mathbb{U}$ of $\mathbb{R}^m$ that maps $\{\mathbf{x}\in\mathbb{R}^m : x_{t+1}=...=x_m=0\}$ into W.

Consider the decomposable form

$$G(\mathbf{X}):=F(\mathbf{X}\,{}^t\mathbb{U}),$$

where we denote $\mathbf{X} := (X_1, \ldots, X_m)$.

We see that $G = L_1' \ldots L_n'$ for linear forms L_i' are linear forms depending only on the variables $X_1, \ldots, X_t$. Note that

$$\mathrm{vol}(F) = |\det \mathbb{U}| \cdot \mathrm{vol}(G) = \mathrm{vol}(G)$$

by the change of variables formula.

For sufficiently small $\delta > 0$, if $|x_i| \leq \delta$ for $i \in \{1, \ldots, t\}$, then

$$|L_i'(\mathbf{x})| \leq 1 \quad \forall i \in \{1, \ldots, n\}.$$

So the set of $\mathbf{x} \in \mathbb{R}^m$ with $|G(\mathbf{x})| \leq 1$ contains the set of $\mathbf{x} \in \mathbb{R}^m$ with $|x_i| \leq \delta$ for $i \in \{1, \ldots, t\}$ and $x_{t+1}, \ldots, x_m$ arbitrary, which has infinite Lebesgue measure. □

Theorem 4.0.3. *Let $F \in \mathbb{Z}[X_1, \ldots, X_m]$ $(m \geq 2)$ be a decomposable form of degree $n > m$ and of finite type. Let S be a finite set of primes and let S' be the subset of all $p \in S$ such that F has a non-trivial zero in $\mathbb{Z}_p^m$. Suppose $s' := \#S' \geq 1$. Then, for all $\varepsilon \in \left(0, \frac{1}{n}\right)$ and $\gamma \in \mathbb{R}_{>0}$, one has*

$$N(F, S, \varepsilon, B, \gamma) \asymp_{F,S,\varepsilon} \gamma^{1/q(F)} \cdot B^{m-(n\varepsilon)/q(F)} (\log B)^{\nu_S^*(F)-1} \quad \text{as } B \to \infty,$$

with implied constants independent of γ, where

$$\nu_S^*(F) := \sum_{p \in S'} \nu_p^*(F) \in \mathbb{Z} \cap [s', (m-1)s'].$$

Proof. The proof follows exactly the same line as the proof of theorem 3.2.1, using theorem 1.3.8, corollary 1.3.5, proposition 2.5.5 and proposition 4.0.1 in place of corollary 1.1.6, corollary 1.2.7, proposition 2.5.3 and proposition 3.1.2 respectively. □

Remark 4.0.4. *If $S' = \emptyset$, then $N(F, S, \varepsilon, B, \gamma)$ is eventually constant as $B \to \infty$.*

Recall that a decomposable form $F \in \mathbb{Z}[X_1, \ldots, X_m]$ has non-zero discriminant (cf. [EG92]) if and only if there exists a factorization $F = L_1 \ldots L_n$ for some linear forms with coefficients over an algebraic closure of $\mathbb{Q}$ such that, for any $I = \{i_1, \ldots, i_l\} \subseteq \{1, \ldots, n\}$ with $1 \leq \#I \leq m$, the linear forms $L_{i_1}, \ldots, L_{i_l}$ are linearly independent over $\overline{\mathbb{Q}}$.

Corollary 4.0.5. *Let $F \in \mathbb{Z}[X_1, \ldots, X_m]$ $(m \geq 2)$ be a decomposable form of degree $n > m$ and non-zero discriminant. Let S be a finite set of primes and let S' be the subset of all $p \in S$ such that F has a non-trivial zero in $\mathbb{Z}_p^m$. Suppose $s' := \#S' \geq 1$. Then, for all $\varepsilon \in \left(0, \frac{1}{n}\right)$ and $\gamma \in \mathbb{R}_{>0}$, one has*

$$N(F, S, \varepsilon, B, \gamma) \asymp_{F,S,\varepsilon} \gamma \cdot B^{m-n\varepsilon}(\log B)^{\nu_S^*(F)-1} \quad \text{as } B \to \infty,$$

with implied constants independent of γ, where

$$\nu_S^*(F) := \sum_{p \in S'} \nu_p^*(F) \in \mathbb{Z} \cap [s', (m-1)s'].$$

Proof. From the fact that F has non-zero discriminant, it follows immediately that $\mathrm{rk}(F) = m$ and $q(F) = 1$. □

Corollary 4.0.6. *Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $n > 2$ and splitting field K over $\mathbb{Q}$. Let S be a finite set of primes and let S' be the subset of all $p \in S$ such that F has a non-trivial zero in $\mathbb{Z}_p^2$. Suppose $s' := \#S' \geq 1$ and denote by $R(F)$ the maximum multiplicity of a linear factor of F in $K[X, Y]$. Then, for all $\varepsilon \in \left(0, \frac{1}{n}\right)$ and $\gamma \in \mathbb{R}_{>0}$, one has*

$$N(F, S, \varepsilon, B, \gamma) \asymp_{F,S,\varepsilon} \gamma^{1/R(F)} \cdot B^{2-(n\varepsilon)/R(f)}(\log B)^{s'-1} \quad \text{as } B \to \infty,$$

with implied constants independent of γ.

Proof. If $L_1, L_2 \in \mathbb{C}[X, Y]$ are two linear forms not multiple of each other, then the intersection of their support is $\{0\}$. Therefore $q(F) = R(F)$ for any binary form $F \in \mathbb{Z}[X, Y]$. □

A final comment

We want to conclude this chapter, and the whole thesis, by pointing out that, in the theoretical perspective, decomposability plays a fundamental role only in the proof of proposition 4.0.1.

Indeed, for any (non necessarily decomposable) form $F \in \mathbb{Z}[X_1, \ldots, X_m]$ $(m \geq 2)$, the definition of $\mathbb{A}(F, S, \varepsilon, B, \gamma)$ still makes sense, and, if F is of finite type, then the results from chapters 1 and 2 yield

$$\mu^m(\mathbb{A}(F, S, \varepsilon, B, \gamma)) \asymp_{F,S,\varepsilon} \gamma^{\mathrm{plct}_{\mathbb{C}}(F)} \cdot B^{m-\mathrm{plct}_{\mathbb{C}}(F)\cdot n\varepsilon} (\log B)^{\nu_S^*(F)-1} \tag{4.8}$$

as $B \to \infty$ (with implied constants independent of γ), where $\mathrm{plct}_{\mathbb{C}}(F)$ denotes the projective log-canonical threshold of F as of definition 1.1.7, and $\nu_S^*(F) = \sum_{p\in S} \nu_p^*(F)$.

Of course, the quantity $\mathrm{plct}_{\mathbb{C}}(F)$ is very difficult to compute in general, so Teitler's result makes the formulation of (4.8) much more practical in the case of decomposable forms (of finite type). Neverthess, the existence of an asymptotic extimate of the form (4.8) does not rely on decomposability.

On the other hand, going through Liu's thesis, one immediately realizes that the upper bound on the asymptotic rate of the difference

$$\left|\#(\mathbb{Z}^m \cap \mathbb{A}(F, S, \varepsilon, B, \gamma)) - \mu^m(\mathbb{A}(F, S, \varepsilon, B, \gamma))\right| \tag{4.9}$$

as $B \to \infty$ that we gave in the case of decomposable forms $F \in \mathbb{Z}[X_1, \ldots, X_m]$ strongly relies on decomposability.

The question whether (or when) the quantity (4.9) is neglegible with respect to $\mu^m(\mathbb{A}(F, S, \varepsilon, B, \gamma))$ as $B \to \infty$ for non-decomposable forms F is certainly very interesting. It seems, however, that addressing such a question would require a significantly different approach.

Acknowledgements

First and foremost, I want to thank that one lady who has always been there for me, giving me the support and relief that I needed in the bad situations – lady Mathematics.

In the last few years, unfortunately, I have been going through some unpleasant personal problems. Had it not been for my deep emotional connection with mathematics, there would not have been any chance of my being writing, right now, the last few lines of this thesis.

On the bright side, the last few years have given me the biggest chance of self-development that I have ever had in my entire life. Experiencing many new situations and interacting with many different kinds of people has certainly helped a lot in this regard, so I want to thank the Algant consortium for the opportunity given to me.

Ringrazio mia mamma Stefania Pierangeli e mia zia Daniela Pierangeli per l'inesauribile supporto emotivo e pratico datomi nei momenti difficili.

I also thank my girlfriend Tata Sheriff for the emotional support and all the amazing tips on coping techniques she has been giving me.

Last, but certainly not least, I want to thank my thesis advisor – Dr. Jan-Hendrik Evertse – for the suggestion of this very interesting problem and the extremely detailed analysis of my work.

Bibliography

[BEG18] Y. Bugeaud, J.-H. Evertse, and K. Győry, *S-parts of values of univariate polynomials, binary forms and decomposable forms at integral points*, Acta Arith. **184** (2018), 151–185.

[Eve92] G. R. Everest, *Uniform distribution and lattice point counting*, J. Austral. Math. Soc. **53** (1992), 39–50.

[EG92] J.-H. Evertse and K. Győry, *Effective finiteness theorems for decomposable forms of given discriminant*, Acta Arith. (1992).

[FS09] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, 2009.

[GV13] S. Gross and A. Vincent, *On the factorization of $f(n)$ for $f(x)$ in $\mathbb{Z}[x]$*, Int. J. Number Theory **9** (2013), 1225–1236.

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag New York, Inc., 1977.

[Igu74] J.-I. Igusa, *Complex powers and asymptotic expansions. I. Functions of certain types*, J. reine und angew. Math. **268–269** (1974), 110–130.

[Kob84] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions (Second Edition)*, Springer-Verlag New York, Inc., 1984.

[Liu15] J. Liu, *On p-adic Decomposable Form Inequalities*, PhD Thesis, Leiden University Repository, 2015.

[Laz04] R. Lazarsfeld, *Positivity in Algebraic Geometry I-II*, Springer-Verlag New York, Inc., 2004.

[Neu99] J. Neukich, *Algebraic Number Theory*, Springer-Verlag New York, Inc., 1999.

[Seg11] D. Segers, *The asymptotic behaviour of the number of solution of polynomial congruences*, An. Şt. Univ. Ovidius Constanţa **19(1)** (2011), 255–262.

[Ste84] C. L. Stewart, *A note on the product of consecutive integers*, Proc. Janos Bolyai Math. Soc. Colloquium on Number Theory **34** (1984), 1523–1527.

[Ste91] ______, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. **4(4)** (1991), 793–835.

[Tei08] Z. Teitler, *A note on Mustaţă computation of multiplier ideals of hyperplane arrangements*, Proc. Amer. Math. Soc. **136(5)** (2008), 1575–1579.

[Thu01] J. L. Thunder, *Decomposable Form Inequalities*, Annals of Mathematics **153(3)** (2001), 767–804.

[VZG08] W. Veys and W. A. Zúñiga-Galindo, *Zeta Functions for Analytic Mappings, Log-Principalization of Ideals, and Newton Polyhedra*, Trans. of the Amer. Math. Soc. **360(4)** (2008), 2205–2227.