Hilbert-Kamke Problem in Number Fields

by

Xingchi Ruan

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2026

© Xingchi Ruan 2026

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner:	Vijaya Kumar Murty Professor, Dept. of Mathematics University of Toronto
Supervisor:	Wentang Kuo Professor, Dept. of Pure Mathematics University of Waterloo
Internal Member:	Matthew Satriano Professor, Dept. of Pure Mathematics University of Waterloo
Internal Member:	Michael Rubinstein Professor, Dept. of Pure Mathematics University of Waterloo
Internal-External Member:	Francis Poulin Professor, Dept. of Applied Mathematics University of Waterloo

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

The Hilbert-Kamke problem asks for the solubility of the system of equations

$$x_1^s + \cdots + x_k^s = N_s, \qquad s = 1, \ldots, n,$$

in natural numbers $x_1, \ldots, x_k$, where $N_1, \ldots, N_n$ are given natural numbers and k is large in terms of n. Over $\mathbb{Q}$, the circle method gives an asymptotic formula for the number of solutions with variables at most P, whose main term is the product of the singular series, the normalized singular integral and $P^{k-\frac{1}{2}n(n+1)}$. So the system is soluble for large $N_1, \ldots, N_n$ when both factors are bounded below by positive constants independent of P and $N_1, \ldots, N_n$. For the normalized singular integral, this holds under a growth condition on the sizes of $N_1, \ldots, N_n$. The lower bound for the singular series is a question about the solubility of the system modulo prime powers, and it holds under an arithmetic condition.

In this thesis, we study the problem over a number field K of degree m, with $N_1, \ldots, N_n$ algebraic integers of K and $x_1, \ldots, x_k$ algebraic integers of K whose images under the embeddings of K into $\mathbb{C}$ are at most P in absolute value. We set up the circle method for the system over K, following Siegel and Wang. The estimate for the minor arcs can be obtained from the work of Wooley, and the lower bound for the normalized singular integral is a question about the real solutions of the system, as over $\mathbb{Q}$. The remaining problem is the singular series σ. We prove that σ converges absolutely for $k > n(n+1)$, that σ is the product of local factors $\sigma_\wp$ over the prime ideals $\wp$ of K, and that the lower bound for σ reduces to non-singular solutions of the system modulo finitely many prime ideal powers. We then bound $\sigma_\wp$ from below by a positive constant independent of $N_1, \ldots, N_n$ for every $\wp$, by reduction to the classical case when $\wp$ is unramified of residue degree one, and otherwise by a direct construction of the solutions in the ring of integers and a lifting one step at a time, for quadratic fields and then for every number field. The main result is that, for $n \geq 3$, σ is bounded below by a positive constant depending only on n and m whenever $N_1, \ldots, N_n$ satisfy an arithmetic condition and $k \geq (n+1)^m n^2 2^{2n-1}$.

Acknowledgements

I thank my supervisor, Professor Wentang Kuo, for suggesting the problem and for his guidance and patience during the preparation of this thesis. I thank the members of my examining committee, Professor Vijaya Kumar Murty, Professor Matthew Satriano, Professor Michael Rubinstein and Professor Francis Poulin, for reading the thesis and for their comments.

Statement on the Use of Generative Artificial Intelligence

Generative artificial intelligence was used in the preparation of this thesis. It was used to check and correct the grammar, to adjust the LaTeX source, the formatting and the layout, and to draft and revise passages of the text at my direction. Everything it produced was read and checked by me, and corrected or rewritten where necessary. I am responsible for the content and accuracy of the whole thesis.

Table of Contents

Examining Committee ii

Author's Declaration iii

Abstract iv

Acknowledgements v

Statement on the Use of Generative Artificial Intelligence vi

List of Symbols x

1 Introduction 1

1.1 Historical Background 1

1.2 The Hilbert-Kamke Problem 2

1.3 The Circle Method 3

1.4 Developments in the Hilbert-Kamke Problem 4

1.5 The Hilbert-Kamke Problem in Number Fields 5

1.6 The Quadratic Case 7

1.7 The General Case 8

2 Waring's Problem **10**

2.1 Waring's Problem and Hilbert's Theorem 10

2.2 The Circle Method 11

2.3 Major and Minor Arcs 11

2.4 The Minor Arcs 12

2.5 The Major Arcs 13

2.6 Lower Bound for $\mathfrak{S}_{s,k}(N)$ 15

2.7 The Asymptotic Formula 16

3 The Hilbert-Kamke Problem in Integers **18**

3.1 The Asymptotic Formula 18

3.2 The Singular Series 20

3.3 An Arithmetic Condition 21

3.4 Result for $p \leq n$ 22

3.5 Result for $p > n$ 22

3.6 Result for $p \geq 9n^2$ 23

3.7 Solubility of the System 24

4 Number Fields **26**

4.1 Number Fields and Rings of Integers 26

4.1.1 Real and Complex Embeddings 27

4.1.2 Norm and Trace 27

4.1.3 Discriminant and Different 28

4.2 The Setup of the Circle Method 28

4.2.1 The Space $K_{\mathbb{R}}$ and the Character E 29

4.2.2 The Counting Function and Its Integral Representation 31

4.2.3 Lemmas 32

4.2.4 Farey Dissection 35

4.3 The Major-Arc Evaluation . . . 37
4.3.1 Gauss Sums and the Singular Series . . . 37
4.3.2 An Approximation Lemma . . . 38
4.3.3 Reduction to the Truncated Singular Series and the Truncated Singular Integral . . . 40
4.4 The Singular Series . . . 42
4.4.1 Bounds for the Gauss Sums and Absolute Convergence . . . 42
4.4.2 The Major-Arc Asymptotic . . . 46
4.4.3 Euler Product and Local Densities . . . 48
4.5 Local Solubility and the Lower Bound for the Singular Series . . . 49

5 The Quadratic Case for $p \leq n$ 54
5.1 Quadratic Fields . . . 54
5.2 The Arithmetic Condition . . . 55
5.3 Split Prime Ideals . . . 58
5.4 Auxiliary Lemmas . . . 61
5.5 Inert and Ramified Prime Ideals . . . 63

6 The General Case 70
6.1 Prime Ideals above $p > n$ . . . 70
6.2 The Arithmetic Condition for a Field of Degree m . . . 74
6.3 Unramified Prime Ideals of Residue Degree One . . . 75
6.4 Prime Ideals above $p \leq n$ . . . 76
6.5 Lower Bound for the Singular Series . . . 77
6.6 Future Work . . . 78

References 80

List of Symbols

The list gives the main symbols in the order in which they are defined, with the place of the definition. Throughout, $\mathbb{N} = \{1, 2, \ldots\}$ is the set of natural numbers, n is the highest exponent of the system, k is the number of variables, $N_1, \ldots, N_n$ are the given numbers in the system, p is a rational prime, and $\wp$ is a prime ideal of $\mathcal{O}_K$ above p. In Section 1.1 and Chapter 2, s is the exponent in Waring's problem, and elsewhere s indexes the equations of the system. The letter ε denotes an arbitrarily small positive number.

$g(s)$	the least k such that every natural number is a sum of k s-th powers of non-negative integers, Section 1.1
$G(s)$	the least k such that every sufficiently large natural number is a sum of at most k s-th powers of natural numbers, Section 1.1
$k_{\min}(n)$, $H(n)$	the least number of variables in the Hilbert-Kamke problem over $\mathbb{Z}$, and its value for $n \geq 12$, determined by Mit'kin, Section 1.4
$e(\alpha)$	$e(\alpha) = e^{2\pi i \alpha}$, Section 2.2
$S(\alpha)$	the exponential sum $\sum_{1 \leq x \leq P} e(\alpha x^s)$ with $P = \lfloor N^{1/s} \rfloor$, Section 2.2
$\mathfrak{M}(q,a)$, $\mathfrak{M}$, $\mathfrak{m}$	the major arcs and the minor arcs of Waring's problem, Section 2.3
$S(q,a)$, $V(\beta)$	the complete exponential sum $\sum_{r=1}^{q} e(ar^s/q)$ and the integral $\int_0^P e(\beta y^s)\, dy$, Section 2.5
$\mathfrak{S}_{s,k}(N)$, $\mathfrak{J}_{s,k}(N)$	the singular series and the singular integral of Waring's problem, Definitions 2.10 and 2.12
$A(q,N)$, σ_p	the terms of $\mathfrak{S}_{s,k}(N)$ and its local factors, Section 2.6; σ_p also denotes the local factors of $\sigma_{\mathbb{Z}}$, Lemma 3.2
$r(\boldsymbol{N}, P)$	the number of solutions of the system with $1 \leq x_i \leq P$, Section 3.1, and with $x_i \in \mathcal{P}(P)$, Definition 4.2
$\sigma_{\mathbb{Z}}$, $\tau_{\mathbb{Z}}$	the singular series and the normalized singular integral of the system over $\mathbb{Z}$, Theorem 3.1
$\lambda(N_1, \ldots, N_n, P)$, λ_0	the largest characteristic of a solution of the real system (3.2), and its lower bound in the growth condition, Section 3.7

$S(\boldsymbol{q}, \boldsymbol{a})$, $V(\boldsymbol{z})$	the complete exponential sum and the integral in the singular series and in the normalized singular integral over $\mathbb{Z}$, Theorem 3.1
$W(d, k)$, $W(\mathfrak{q}, k)$	the number of solutions of the system modulo d, Section 3.2, and modulo an integral ideal $\mathfrak{q}$, Definition 4.23
T_1	$T_1 = W(p, k)$ for $p > n$, Section 3.5
$\Gamma_n(\mathbb{Z})$	the set of $\mathbb{Z}$-linear combinations of the vectors $(x, x^2, \dots, x^n)$, $x \in \mathbb{Z}$, Section 3.3
$\varkappa$, δ	for a prime $p \le n$, $p^{\varkappa} \le n < p^{\varkappa+1}$ and $\delta = v_p\big((n-1)!\big)$, Lemma 3.4
$c_*^{\mathbb{Q}}$	the constant $p^{(2\varkappa+2\delta+1)(n-k_1)}$ of Lemma 3.4, also the constant in Theorems 5.8 and 6.8
k_1, k_2	$k_1 = n^2 2^{2n-1}$ and $k_2 = \lfloor 32n^2 \ln n \rfloor + n$, Lemma 3.4 and Section 3.5
K, m, $\mathcal{O}_K$	a number field, its degree and its ring of integers, Section 4.1
$\omega_1, \dots, \omega_m$	an integral basis of $\mathcal{O}_K$, Section 4.1
ι_i, $\alpha^{(i)}$, r_1, r_2	the embeddings of K into $\mathbb{C}$, the images $\alpha^{(i)} = \iota_i(\alpha)$, and the numbers of real embeddings and of pairs of complex embeddings, Section 4.1.1
$N_{K/\mathbb{Q}}$, $\mathrm{Tr}_{K/\mathbb{Q}}$, $N(\mathfrak{a})$	the norm, the trace, and the norm of an integral ideal, Section 4.1.2
Δ_K, D, $\mathfrak{D}$	the discriminant of K, also written D, and the different, Section 4.1.3
$K_{\mathbb{R}}$, $\mathrm{Tr}(\xi)$, $E(\xi)$, $\|\xi\|$	the real algebra of K, the trace $\mathrm{Tr}(\xi) = \sum_i \xi^{(i)}$, the character $E(\xi) = e(\mathrm{Tr}(\xi))$, and $\|\xi\| = \max_i \lvert\xi^{(i)}\rvert$, Section 4.2.1
$\rho_1, \dots, \rho_m$, U_m, $\mathbb{T}$	the dual basis of the integral basis, the fundamental domain of $K_{\mathbb{R}}/\mathfrak{D}^{-1}$, and the torus $(K_{\mathbb{R}}/\mathfrak{D}^{-1})^n$, Section 4.2.1
dx, $d\boldsymbol{x}$, $d\xi$	the Haar measure on $K_{\mathbb{R}}$ in the dual-basis coordinates of the variable of integration, with $\int_{U_m} dx = 1$, its product on $K_{\mathbb{R}}^n$, and the Haar measure in the integral-basis coordinates, which gives $\mathcal{O}_K$ covolume 1, Section 4.2.1
$\gamma \to \mathfrak{a}$, $\mathfrak{a}_{\boldsymbol{\gamma}}$	the denominator of $\gamma \in K$ and the common denominator of $\boldsymbol{\gamma} \in K^n$, Definition 4.1
$\mathcal{P}(P)$, $\mathfrak{B}(P)$	the totally positive integers of K with $\lvert x^{(i)}\rvert \le P$, and the corresponding box in $K_{\mathbb{R}}$, Definition 4.2
$S(\boldsymbol{\alpha}, P)$	the exponential sum over $\mathcal{P}(P)$, Definition 4.4
$d(\mathfrak{a})$, $\#\{\wp \mid \mathfrak{a}\}$	the number of integral ideals dividing $\mathfrak{a}$, Lemma 4.5, and the number of distinct prime ideals dividing $\mathfrak{a}$, Lemma 4.6

$\mathcal{G}_{\mathfrak{q}}$	the group $\mathfrak{q}^{-1}\mathfrak{D}^{-1}/\mathfrak{D}^{-1}$ of order $N(\mathfrak{q})$, Lemma 4.5
θ, t, κ, T', c_0, $\mathbf{\Gamma}(t)$, Ω	the parameters of the Farey dissection, $\theta = 1/(2(m(n+2)+1))$, $t = P^{\theta}$, $T' = t^{\kappa}$ with $0 < \kappa \leq 1$, $c_0 = \frac{1}{2}\lvert D\rvert^{-1/m}$, the set of rational points with denominator of norm at most t^m, and the box (4.4), Section 4.2.4
$\mathbf{B}_{\boldsymbol{\gamma}}$, $\mathbf{B}$, $\mathfrak{m}$	the basic domains, the major arcs and the minor arcs over K, Definitions 4.7 and 4.9
Q, η	$Q = m\big(k - \frac{n(n+1)}{2}\big)$ and $\eta = \frac{k}{n} - n - 1$, Section 4.3
$G(\boldsymbol{\gamma})$, $A(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$	the Gauss sum and the terms of the singular series over K, Definitions 4.11 and 4.12
$\sigma_K = \sigma$, $\sigma(t)$	the singular series of the system over K, written σ from Chapter 4 on, and the truncated singular series, the partial sum of σ over the rational points in $\mathbf{\Gamma}(t)$, Definition 4.12
$E_{\boldsymbol{\beta}}(\xi)$, $V(\boldsymbol{\beta})$, $V_1(\boldsymbol{\beta}')$	the function $E\big(\sum_s \beta_s \xi^s\big)$, Lemma 4.14, the integral approximating $S(\boldsymbol{\alpha}, P)$, Definition 4.13, and its normalized form, Section 4.3.3
ϑ_s, τ_K, J_0	$\vartheta_s = N_s P^{-s}$, the normalized singular integral over K, Definition 4.15, and the truncated singular integral, Theorem 4.21
δ_0	the exponent in the error term of Theorem 4.21
$\sigma_{\wp}$	the local factor of σ at $\wp$, $\sigma_{\wp} = \lim_{h\to\infty} N(\wp)^{h(n-k)} W(\wp^h, k)$, Theorem 4.24
$\mathcal{O}_{\wp}$, $v_{\wp}$, v_p	the completion of $\mathcal{O}_K$ at $\wp$, Section 4.5, the $\wp$-adic valuation on K, Section 4.2.3, and the p-adic valuation on $\mathbb{Q}$, Section 2.6
$J(\boldsymbol{x}, i_1, \ldots, i_n)$, $\ell(\boldsymbol{x})$	the Jacobian minors of a solution and its level, the least valuation of a minor, Definition 4.26
C	the constant of Lemma 4.29 and Theorem 4.30
d, ω, Φ	for a quadratic field, $K = \mathbb{Q}(\sqrt{d})$, $\mathcal{O}_K = \mathbb{Z}[\omega]$, and Φ is the minimal polynomial of ω, Section 5.1
$\wp'$, c	the second prime ideal above a split prime p, and a root of Φ modulo p, Proposition 5.1
$t_r(X)$, $t_{r,l}$	the polynomials $\binom{X}{r}\binom{n-X}{n-r}$ and the integers $t_r(a)t_l(b)$ attached to $x = a + b\omega$, Section 5.2
$\Gamma_n(\mathcal{O}_K)$, Condition (M)	the subgroup of $\mathcal{O}_K^n$ generated by the vectors $(x, x^2, \ldots, x^n)$, $x \in \mathcal{O}_K$, and the condition $(N_1, \ldots, N_n) \in \Gamma_n(\mathcal{O}_K)$, Definition 5.3

ϕ_h, c_h, $c_{i,h}$	the isomorphism $\mathbb{Z}/p^h\mathbb{Z} \to \mathcal{O}_K/\wp^h$ for an unramified prime ideal of residue degree one, and the integers with $\omega \equiv c_h$, respectively $\omega_i \equiv c_{i,h} \pmod{\wp^h}$, Lemma 5.5 and Theorem 6.8
$\tilde{N}_s$, $\hat{N}_s$	the images of N_s in $\mathbb{Z}/p^h\mathbb{Z}$, and the natural numbers that replace them, Lemmas 5.6 and 5.7
e, f, q	the ramification index and the residue degree of $\wp$, and $q = N(\wp) = p^f$, Section 5.4
ϖ, R	a uniformizer $\varpi \in \wp \setminus \wp^2$ and a complete residue system modulo $\wp$, Section 5.4
$\mathcal{S}$	a set of n-tuples $(N_1, \dots, N_n)$, Lemma 5.12
F, χ	the residue field $\mathcal{O}_K/\wp$, Section 6.1, and a non-trivial additive character of the finite field F, Lemma 6.1
$W(\wp^h, k; N_1', \dots, N_n')$	the counting function of the system with $N_1', \dots, N_n'$ in place of $N_1, \dots, N_n$, Section 5.4
W_1	the number of solutions modulo $\wp$ with n pairwise incongruent coordinates, Lemma 6.3
G	the set of non-zero points $r + l\omega$ for a quadratic field, Section 5.5, and of the points $g_{\boldsymbol{r}}$ in general, Section 6.2
α, β, α_0	the parameters of the lifting, (5.7), and $\alpha_0 = 2\varkappa + 2\delta + 1$, the value of α for $e = 1$, Section 5.5
$\Lambda_r(X)$, $\lambda(r, s)$	the Lagrange polynomials for $x_1, \dots, x_n$ and their coefficients, Lemma 5.13
w_s, η_r	the numbers with $N_s - \sum_i x_i^s \equiv \varpi^{\alpha_j} w_s \pmod{\wp^{\alpha_j+1}}$ and the corrections (5.9) in the lifting, Lemma 5.14
k_1', c_*'	$k_1' = (n+1)^2 n^2 2^{2n-1}$ and the constant in Theorem 5.17
$t_{\boldsymbol{r}}$, $g_{\boldsymbol{r}}$	the integers and the points attached to $x = a_1\omega_1 + \cdots + a_m\omega_m$, Lemma 6.6
k_0	the number of variables in Propositions 5.16 and 6.9
k_3, c_*^{gen}	$k_3 = (n+1)^m n^2 2^{2n-1}$, the number of variables, and c_*^{gen}, the constant, in Theorem 6.10; k_3 is also the bound in Theorem 6.11
$\pi(n)$	the number of primes $p \le n$, Theorem 6.11

Chapter 1

Introduction

1.1 Historical Background

The Hilbert-Kamke problem is a topic in additive number theory and a generalization of Waring's problem. Waring's problem asks whether, for every integer $s \geq 2$, there exists $k = k(s)$ such that every natural number $N \in \mathbb{N} = \{1, 2, \ldots\}$ is a sum of k s-th powers of non-negative integers $x_1, \ldots, x_k$,

$$N = x_1^s + x_2^s + \cdots + x_k^s.$$

The Hilbert-Kamke problem extends this question to a system of equations. It asks whether there exists $k = k(n)$, depending only on n, such that for all sufficiently large $N_1, \ldots, N_n$ satisfying certain conditions, which are given in Section 1.2, there exist natural numbers $x_1, \ldots, x_k$ with

$$x_1^s + x_2^s + \cdots + x_k^s = N_s, \qquad s = 1, 2, \ldots, n,$$

that is, whether $N_1, \ldots, N_n$ are simultaneously the sums of the s-th powers, $s = 1, 2, \ldots, n$, of the same k variables.

In 1770, Waring conjectured that such a k exists for every s [26]. Let $g(s)$ denote the smallest such k, if it exists. For example, $g(2) = 4$ and $g(3) = 9$ [8, 28]. Hilbert proved in 1909 that $g(s)$ exists for every s [9]. The exact value of $g(s)$ is known for all s except possibly finitely many, namely

$$g(s) = 2^s + \lfloor (3/2)^s \rfloor - 2;$$

see the survey of Vaughan and Wooley [22]. The lower bound $g(s) \geq 2^s + \lfloor (3/2)^s \rfloor - 2$ is obtained from the number $2^s \lfloor (3/2)^s \rfloor - 1$. This number is less than 3^s, so it can only be represented by the s-th powers 1 and 2^s, and such a representation needs at least $2^s + \lfloor (3/2)^s \rfloor - 2$ terms. Thus the value of $g(s)$ is determined by the representations of small numbers, and it gives no information on the number of s-th powers needed for larger numbers, which usually require far fewer s-th powers. For this reason, one considers $G(s)$, the least k such that every sufficiently large natural number is a sum of at most k s-th powers of natural numbers. Clearly $G(s) \leq g(s)$, and the known upper bounds for $G(s)$ are much smaller than $g(s)$. The value of $G(s)$ is known only for $s = 2$ and $s = 4$, namely $G(2) = 4$ and $G(4) = 16$, and the determination of $G(s)$ remains open for all other s [22].

1.2 The Hilbert-Kamke Problem

Hilbert proposed the following generalization of Waring's problem [9], in which the sums of the first n powers of the same variables are all given, and Kamke solved it in 1921 [12]. The problem is now called the Hilbert-Kamke problem.

Given natural numbers $N_1, N_2, \ldots, N_n$, the Hilbert-Kamke problem asks whether, for k sufficiently large in terms of n, there exist natural numbers $x_1, x_2, \ldots, x_k$ such that

$$\begin{aligned} x_1 + x_2 + \cdots + x_k &= N_1, \\ x_1^2 + x_2^2 + \cdots + x_k^2 &= N_2, \\ &\vdots \\ x_1^n + x_2^n + \cdots + x_k^n &= N_n. \end{aligned}$$

Unlike Waring's equation, this system might not be soluble for arbitrary $N_1, \ldots, N_n$. For every integer x, the vector $(x, x^2, \ldots, x^n)$ is a $\mathbb{Z}$-linear combination of the n vectors $(r, r^2, \ldots, r^n)$, $1 \leq r \leq n$, with the coefficients $\binom{x}{r}\binom{n-x}{n-r}$ (Lemma 3.3). Hence, if the system has a solution, then there exist integers $t_1, \ldots, t_n$ such that

$$(N_1, \ldots, N_n) = \sum_{i=1}^{k} (x_i, x_i^2, \ldots, x_i^n) = \sum_{r=1}^{n} t_r \, (r, r^2, \ldots, r^n).$$

So the system can have a solution only if $(N_1, \ldots, N_n)$ has this form for some integers $t_1, \ldots, t_n$. We call this condition the *arithmetic condition*. It is condition (8.5) of [3, p. 320], and it is stated as condition (3.1) in Chapter 3. Over a number field, the coefficients $\binom{x}{r}\binom{n-x}{n-r}$ are in general not algebraic integers, and the arithmetic condition is stated with

more vectors; see Definition 5.3 in Chapter 5. The sizes of $N_1, \dots, N_n$ are also restricted. For natural numbers $x_1, \dots, x_k$, the power mean inequality and the non-negativity of the x_i give

$$k^{1-s} N_1^s \;\le\; N_s \;\le\; N_1^s, \qquad s = 1, \dots, n,$$

so the numbers $N_1, \dots, N_n$ cannot have arbitrary sizes. In Chapter 3, the solutions are counted in natural numbers $x_1, \dots, x_k \le P$, where P is a parameter. Every solution has $x_i \le N_1$, so the choice $P = N_1$ counts all solutions. The condition on the sizes of $N_1, \dots, N_n$ is a condition on the numbers $N_s P^{-s}$, $s = 1, \dots, n$. It is stated in Section 3.7, following [3, Theorem 8.3, p. 352], and we call it the *growth condition*. In this thesis, we assume the growth condition and study the arithmetic condition.

1.3 The Circle Method

The circle method is an analytic method for counting the solutions of Diophantine equations. Hardy and Ramanujan used it first, for the partition function [7]. Hardy and Littlewood developed it in the series *Partitio Numerorum* [6] and applied it to Waring's problem. The counting function is written as an integral of a power of an exponential sum over the unit interval. The interval is divided into major and minor arcs. The major arcs give the main term of an asymptotic formula, and the minor arcs give the error term. The main term is a product of two factors, the singular series and the singular integral. The singular series is a sum over the reduced fractions a/q in $(0, 1]$. It is determined by the solutions of the equation modulo every integer. The singular integral is determined by the real solutions of the equation. Chapter 2 presents this method for Waring's problem.

The circle method gives an asymptotic formula for the number of solutions of the Hilbert-Kamke system in natural numbers $x_1, \dots, x_k \le P$, for k large in terms of n. The main term of the formula is $\sigma_{\mathbb{Z}} \tau_{\mathbb{Z}} P^{k - \frac{1}{2}n(n+1)}$, where $\sigma_{\mathbb{Z}}$ is the singular series, $\tau_{\mathbb{Z}}$ is the normalized singular integral, and $P^{k-\frac{1}{2}n(n+1)}$ is the expected size of the number of solutions; the formula is stated in Chapter 3. The series $\sigma_{\mathbb{Z}}$ depends on $N_1, \dots, N_n$, and $\tau_{\mathbb{Z}}$ depends on $N_1, \dots, N_n$ and P. The system has a solution for large P if they are bounded below by positive constants independent of P and $N_1, \dots, N_n$. The two conditions of Section 1.2 correspond to the two factors. Under the growth condition, which is a condition on the numbers $N_s P^{-s}$ (Section 3.7), $\tau_{\mathbb{Z}}$ is bounded below by a positive constant independent of P and $N_1, \dots, N_n$ (Lemma 3.10). The singular series $\sigma_{\mathbb{Z}}$ is, for k large enough, a product of local factors σ_p over the primes p, and σ_p is the density of solutions of the system modulo the powers of p. So the lower bound for $\sigma_{\mathbb{Z}}$ depends on the solubility of the system modulo prime powers, that is, on its local solubility. The arithmetic condition is necessary for $\sigma_{\mathbb{Z}}$

to be bounded below by a positive constant [3, p. 338], and for $k \geq \max(k_1, k_2)$, where $k_1 = n^2 2^{2n-1}$ and $k_2 = \lfloor 32n^2 \ln n \rfloor + n$, it gives $\sigma_{\mathbb{Z}} \geq n^{-20n^4 2^n}$, which is independent of $N_1, \ldots, N_n$ (Theorem 3.9). The asymptotic formula itself needs an estimate for the minor arcs. Over $\mathbb{Q}$, Wooley [30, Theorem 1.1] proves the asymptotic formula for $n \geq 3$ and $k \geq n(n+1)$, under the assumption of local solubility, so we do not treat the minor arcs in this thesis; see Remark 4.10 in Chapter 4. We assume the growth condition and therefore resolve the problem of the uniform lower bound for the singular integral. The remaining problem is the singular series, which is reduced to the local solubility of the system, that is, to the lower bound for $\sigma_{\mathbb{Z}}$ under the arithmetic condition.

Vinogradov gave stronger estimates for the exponential sums in the circle method [24], and with them the method was applied to systems of equations. Arkhipov, Chubarikov and Karatsuba studied systems of equations in power sums, including the Hilbert-Kamke system [1, 2, 3]. Their book [3] is the source of the classical results in Chapter 3.

1.4 Developments in the Hilbert-Kamke Problem

Mardzhanishvili in 1937 gave a condition on $N_1, \ldots, N_n$ that is necessary for the solubility of the system [16], and showed that under this condition the singular series is positive for $k > 2^{n^2-n-2} n^4$. Arkhipov gave necessary and sufficient conditions for the positivity of the singular series [1, 2].

Let $k_{\min}(n)$ be the least k such that the Hilbert-Kamke system is soluble in natural numbers for all sufficiently large $N_1, \ldots, N_n$ that satisfy the growth condition and the arithmetic condition of Section 1.2, as in the definition of $G(s)$. Mit'kin determined the values of $k_{\min}(n)$ for $n \geq 12$. He proved in [17] that $k_{\min}(n) \leq H(n)$ and in [18] that $k_{\min}(n) \geq H(n)$, so that

$$k_{\min}(n) = H(n), \qquad H(n) = \sum_{0 \leq j \leq \left\lfloor \frac{\ln n}{\ln 2} \right\rfloor} 2^j \left(2^{\lfloor n/2^j \rfloor} - 1\right) \quad (n \geq 12).$$

For every $n \geq 3$, $k_{\min}(n) \geq 2^n - 1$ [3, Lemma 8.10 and Theorem 8.2, pp. 341–343]. So $k_{\min}(n)$ is known for the integers when $n \geq 12$. In this thesis, we focus on upper bounds for the corresponding number over the ring of integers of a number field.

1.5 The Hilbert-Kamke Problem in Number Fields

We now state the Hilbert-Kamke problem in number fields. Let K be a number field of degree m with ring of integers $\mathcal{O}_K$. For algebraic integers $N_1, \dots, N_n \in \mathcal{O}_K$, we ask for solutions $x_1, \dots, x_k \in \mathcal{O}_K$ of the system

$$\begin{aligned} x_1 + \cdots + x_k &= N_1, \\ &\vdots \\ x_1^n + \cdots + x_k^n &= N_n. \end{aligned}$$

Over $\mathbb{Q}$, the variables run over the natural numbers up to P. Over K, the variables cannot run over all algebraic integers $x \in \mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(x)| \leq P$, because this set is infinite when $\mathcal{O}_K$ has infinitely many units. Following Siegel [19, 20] and Wang [25, Chapter 5], we let the variables run over the algebraic integers of K whose images under the embeddings of K into $\mathbb{C}$ are all at most P in absolute value and positive at every real embedding. This set is denoted $\mathcal{P}(P)$ and defined in Chapter 4 (Definition 4.2). It is finite, $\#\mathcal{P}(P) \asymp P^m$, and it replaces $\{1, \dots, P\}$. If the system has a solution in $\mathcal{P}(P)$, then N_s is totally positive, that is, positive at every real embedding, and all its images under the embeddings are at most kP^s in absolute value.

As over $\mathbb{Q}$, two conditions on $N_1, \dots, N_n$ enter, an arithmetic condition and a growth condition. The arithmetic condition over K is Condition (M) of Definition 5.3. It has the same form as condition (3.1), with the n points $1, \dots, n$ replaced by the $(n+1)^m - 1$ points of $\mathcal{O}_K$ in Lemma 6.7, because for $x \in \mathcal{O}_K$ the coefficients $\binom{x}{r}\binom{n-x}{n-r}$ are in general not algebraic integers. The growth condition over K is a condition on the solutions of the system in the real algebra $K_{\mathbb{R}}$ of K (Chapter 4), similar to the case of $\mathbb{Q}$ (Section 4.4.2). Under these two conditions, the circle method applies to the system over K as over $\mathbb{Q}$.

Siegel [19, 20] introduced the circle method over number fields and used it for Waring's problem over K. Wang [25] wrote a book on the circle method over number fields, in which he studies a single equation. We follow Siegel and Wang, and we set up the circle method for the Hilbert-Kamke system over K in Chapter 4. The number of solutions in $\mathcal{P}(P)$ is written as an integral of a power of an exponential sum over a torus of dimension mn, which replaces the unit cube $[0,1]^n$ of Chapter 3. The torus is divided into major arcs and minor arcs. The minor arcs give the error term. Their estimate can be obtained from the work of Wooley (Remark 4.10), so we do not treat it in this thesis. The major arcs give the main term $\sigma_K \tau_K P^Q$, where σ_K is the singular series of the system, τ_K is the normalized singular integral and $Q = m\big(k - \frac{1}{2}n(n+1)\big)$ (Section 4.4.2). As over $\mathbb{Q}$, the two conditions correspond to the two factors. Over $\mathbb{Q}$, Arkhipov, Chubarikov and Karatsuba bound $\tau_{\mathbb{Z}}$

below by a positive constant independent of P and $N_1, \dots, N_n$ under the growth condition (Lemma 3.10), and the same argument gives such a bound for τ_K (Section 4.4.2). With the singular integral and the minor arcs dealt with in this way, the remaining problem is the lower bound for σ_K under the arithmetic condition, and it is the subject of this thesis.

The singular series σ_K is defined in Chapter 4 as a sum over the n-tuples of ideals of $\mathcal{O}_K$ (Definition 4.12). For a non-zero ideal $\mathfrak{q}$ of $\mathcal{O}_K$ and $x_1, \dots, x_k$ running over a complete residue system modulo $\mathfrak{q}$, we define $W(\mathfrak{q}, k)$ as the number of solutions of the system of congruences

$$x_1^s + \cdots + x_k^s \equiv N_s \pmod{\mathfrak{q}}, \quad s = 1, \dots, n.$$

Chapter 4 proves the following theorem.

Theorem (Theorem 4.20, Lemma 4.22 and Theorem 4.24)**.** *Let $n \geq 2$ and $k > n(n+1)$. Then σ_K converges absolutely, and*

$$\sigma_K = \prod_{\wp} \sigma_\wp, \qquad \sigma_\wp = \lim_{h \to \infty} N(\wp)^{h(n-k)} W(\wp^h, k),$$

where the product runs over the prime ideals of $\mathcal{O}_K$.

The factor $\sigma_\wp$ is the density of solutions of the system modulo the powers of $\wp$. So the size of σ_K depends on the solubility of the system modulo every power of every prime ideal. The main result of Chapter 4 is the following theorem. It reduces the lower bound for σ_K to finitely many prime ideals. Non-singular solutions are defined in Section 4.5.

Theorem (Theorem 4.30)**.** *Let $n \geq 2$ and $k > n(n+1)$. There is a constant $C = C(n, m, k)$ such that the following holds. If, for every prime ideal $\wp$ with $N(\wp) \leq C$, there is an integer $\ell_\wp \geq 0$ such that the system modulo $\wp^{2\ell_\wp + 1}$ has a non-singular solution of level $\ell_\wp$, then*

$$\sigma_K \;\geq\; c_1 \prod_{N(\wp) \leq C} N(\wp)^{-(2\ell_\wp+1)(k-n)} \;>\; 0, \qquad c_1 = \prod_{N(\wp) > C} \left(1 - N(\wp)^{-1-\eta/2}\right) > 0,$$

where $\eta = k/n - n - 1$, and $c_1 = c_1(K, n, k)$ depends on K.

The setup in Chapter 4 follows Siegel and Wang. The results on the convergence of σ_K, the product formula and Theorem 4.30 are new. The results of Chapters 5 and 6 are lower bounds of the form $W(\wp^h, k) \geq c_\wp N(\wp)^{h(k-n)}$, with $c_\wp$ bounded below by a positive constant independent of $N_1, \dots, N_n$, for every prime ideal $\wp$, and in particular for the prime ideals with $N(\wp) \leq C$.

Let $\wp$ be a prime ideal above the rational prime p. The two cases are $p > n$, where $p \nmid n!$, and $p \le n$, where $p \mid n!$. For $p > n$, the number $n!$ is a unit modulo $\wp$. The solutions of the system modulo $\wp$ are counted by a character sum over the residue field $\mathcal{O}_K/\wp$, and they are lifted to the powers of $\wp$ by Hensel's lemma. This argument needs no condition on $N_1, \dots, N_n$, and it is the same for every number field, so it is given once, in Chapter 6. For $p \le n$, the number $n!$ lies in $\wp$, the standard (non-singular) form of Hensel's lemma does not apply, and the solutions are constructed from Condition (M) and lifted step by step. The construction depends on the prime ideal. Chapter 5 gives it for quadratic fields, where $m = 2$, and Chapter 6, for an arbitrary number field.

1.6 The Quadratic Case

The local analysis is done one prime ideal at a time. We consider quadratic fields first, because this special case illustrates the method in detail and shows how it generalizes to an arbitrary number field: every step can be written with explicit elements and explicit prime ideals, and the three kinds of prime ideals of a quadratic field are the simplest instances of the three cases that occur in an arbitrary number field. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 0, 1$ a square-free integer. The ring of integers is $\mathbb{Z}[\omega]$ with $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ and $\omega = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$. The prime ideals of $\mathcal{O}_K$ fall into three kinds, split, inert and ramified, depending on the factorization of the minimal polynomial of ω modulo p (Proposition 5.1): for a split prime ideal $\mathcal{O}_K/\wp^h \cong \mathbb{Z}/p^h\mathbb{Z}$, for an inert prime ideal $|\mathcal{O}_K/\wp| = p^2$, and for a ramified prime ideal $v_\wp(p) = 2$. Chapter 5 considers the prime ideals above the primes $p \le n$, which need Condition (M). The prime ideals above $p > n$ are considered in Chapter 6 for every number field; see Section 1.5.

For a split prime ideal $\wp$, the quotients $\mathcal{O}_K/\wp^h$ are isomorphic to $\mathbb{Z}/p^h\mathbb{Z}$, and the isomorphism reduces the counting problem to the classical one. We will prove the following theorem.

Theorem (Theorem 5.8)**.** *Let $n \ge 3$, let K be a quadratic field with ring of integers $\mathbb{Z}[\omega]$, let $p \le n$ be a prime, and let $\wp = (p, \omega - c)$ be a split prime ideal of $\mathcal{O}_K$, where c is a root of the minimal polynomial of ω modulo p. Suppose that $N_1, \dots, N_n$ satisfy Condition* (M)*. Then, for $k \ge k_1 = n^2 2^{2n-1}$ and every $h \ge 1$,*

$$W(\wp^h, k) \;\ge\; c_*^{\mathbb{Q}}\, N(\wp)^{h(k-n)}, \qquad c_*^{\mathbb{Q}} = p^{(2\varkappa+2\delta+1)(n-k_1)},$$

where $p^\varkappa \le n < p^{\varkappa+1}$ and $\delta = v_p\big((n-1)!\big)$. Hence $\sigma_\wp \ge c_*^{\mathbb{Q}} > 0$.

There is no such isomorphism for the inert and the ramified prime ideals, and the classical construction does not apply. For an inert prime ideal, $|\mathcal{O}_K/\wp^h| = p^{2h}$, while the image of $\mathbb{Z}$ in $\mathcal{O}_K/\wp^h$ has p^h elements. For a ramified prime ideal $\wp$ of a quadratic field, $v_\wp(a) = 2v_p(a)$ for every non-zero integer a, where $v_\wp$ and v_p are the $\wp$-adic and the p-adic valuations. In both cases, we construct the solutions in $\mathcal{O}_K$ directly. The construction uses the identity

$$x^s = \sum_{g \in G} t_g \, g^s, \qquad s = 1, \ldots, n,$$

which holds for every $x \in \mathcal{O}_K$ with integers t_g depending on x, where G is the set of the $(n+1)^2 - 1$ non-zero numbers $r + l\omega$ with $0 \le r, l \le n$ (Lemma 5.2), and a lifting that takes a solution of the system modulo $\wp^{\alpha+j}$ to a solution modulo $\wp^{\alpha+j+1}$ for $j = 0, 1, 2, \ldots$, where α is a fixed exponent (Lemma 5.14). The lifting runs over the powers of a uniformizer of $\wp$, which is p in the inert case, and it is written so that it applies to every prime ideal of every number field. We will prove the following theorem, in which the bound does not depend on p.

Theorem (Theorem 5.17)**.** *Let $n \ge 3$, let K be a quadratic field, let $\wp$ be an inert or a ramified prime ideal of $\mathcal{O}_K$ above a rational prime $p \le n$, and suppose that $N_1, \ldots, N_n$ satisfy Condition* (M)*. Let $k_1' = (n+1)^2 n^2 2^{2n-1}$. Then, for $k \ge k_1'$ and every $h \ge 1$,*

$$W(\wp^h, k) \;\ge\; c_*' \, N(\wp)^{h(k-n)}, \qquad c_*' = \left(n^2 2^{2n-1}\right)^{2(n-k_1')}.$$

Hence $\sigma_\wp \ge c_*' > 0$.

1.7 The General Case

With the detailed calculations of Chapter 5 as examples, Chapter 6 extends the results of Chapter 5 to a number field K of arbitrary degree m. It begins with the prime ideals above $p > n$. The solutions modulo $\wp$ are counted by a character sum over the residue field $\mathcal{O}_K/\wp$ and lifted by Hensel's lemma, and Condition (M) is not needed (Theorem 6.5). For the prime ideals above $p \le n$, Condition (M) is needed, and its $(n+1)^m - 1$ points $r_1\omega_1 + \cdots + r_m\omega_m$, $0 \le r_i \le n$, not all zero, replace the $(n+1)^2 - 1$ points $r + l\omega$ of the quadratic case, where $\omega_1, \ldots, \omega_m$ is an integral basis, so the number of variables grows with the degree. Let e be the ramification index and f the residue degree of a prime ideal $\wp$ above p, so that $v_\wp(p) = e$ and $|\mathcal{O}_K/\wp| = p^f$. For the unramified prime ideals of residue degree one, the reduction to the classical problem is the same as in the quadratic case, and the lifting of Chapter 5 applies to the other prime ideals above $p \le n$ without change. The main theorem of the thesis is the following.

Theorem (Theorem 6.11)**.** *Let $n \geq 3$, and let K be a number field of degree m. Suppose that $N_1, \dots, N_n$ satisfy Condition* (M) *of Definition 5.3 and that*

$$k \;\geq\; k_3 \;=\; (n+1)^m\, n^2 2^{2n-1}.$$

Then

$$\sigma_K \;\geq\; \exp\big(-2m\zeta(3)\big)\,\big(c_*^{\mathrm{gen}}\big)^{m\pi(n)}\Big(\prod_{n<p<9n^2} p\Big)^{-mk_2} \;>\; 0,$$

where $c_*^{\mathrm{gen}} = \big(n^2 2^{2n-1}\big)^{m(n-k_3)}$, $k_2 = \lfloor 32n^2 \ln n \rfloor + n$, $\pi(n)$ is the number of primes $p \leq n$, and $\zeta(3) = \sum_{j\geq 1} j^{-3}$.

The lower bound for σ_K does not depend on $N_1, \dots, N_n$.

Chapter 2

Waring's Problem

This chapter reviews the circle method as developed by Hardy and Littlewood for Waring's problem. The definitions and theorems follow the book of Vaughan [21], and we refer to it for the proofs.

2.1 Waring's Problem and Hilbert's Theorem

Recall that Waring's problem asks whether, for every integer $s \geq 2$, there is $k = k(s)$ such that every natural number is a sum of k s-th powers of non-negative integers. Write $g(s)$ for the least such k. Write $G(s)$ for the least k such that every sufficiently large natural number N is a sum of at most k s-th powers of natural numbers. Clearly $G(s) \leq g(s)$.

Theorem 2.1 (Hilbert [9])**.** *For every $s \geq 2$, the number $g(s)$ is finite.*

Proof. See [9]. □

In [9], Hilbert did not provide an explicit bound for $g(s)$, and therefore none for $G(s)$. The first explicit bound, $G(s) \leq (s-2)2^{s-1}+5$, was obtained by Hardy and Littlewood with the circle method; see [22, Section 3]. The form of the method presented in this chapter, which uses Hua's lemma, gives an asymptotic formula for the number of representations of N as a sum of k s-th powers when $k \geq 2^s + 1$, and hence $G(s) \leq 2^s + 1$. Vinogradov's method of estimating exponential sums reduces the number of variables required, and gives $G(s) \leq 32(s \ln s)^2$ [23].

2.2 The Circle Method

For $\alpha \in \mathbb{R}$, let $e(\alpha) = e^{2\pi i\alpha}$. Then $e(\alpha)e(\beta) = e(\alpha+\beta)$, and, for $h \in \mathbb{Z}$, we have the orthogonality relation

$$\int_0^1 e(\alpha h)\, d\alpha = \begin{cases} 1, & h = 0, \\ 0, & h \in \mathbb{Z} \setminus \{0\}. \end{cases}$$

Fix $s \geq 2$ and $k \in \mathbb{N}$. For $N \in \mathbb{N}$, let $R_{s,k}(N)$ be the number of solutions in natural numbers $x_1, \ldots, x_k$ of

$$N = x_1^s + x_2^s + \cdots + x_k^s.$$

Necessarily $x_i \leq N^{1/s}$. Define $P = \lfloor N^{1/s} \rfloor$ and

$$S(\alpha) = \sum_{1 \leq x \leq P} e\big(\alpha x^{\,s}\big).$$

Expanding the k-th power of $S(\alpha)$ and using orthogonality,

$$\int_0^1 S(\alpha)^{\,k} e(-N\alpha)\, d\alpha = \sum_{1 \leq x_1, \ldots, x_k \leq P} \int_0^1 e\big(\alpha(x_1^s + \cdots + x_k^s - N)\big)\, d\alpha = R_{s,k}(N),$$

and we estimate this integral. The unit interval is divided into two parts, the major arcs, which are neighbourhoods of rational numbers with small denominators and give the main term, and the minor arcs, which form the rest of the interval and give the error term.

2.3 Major and Minor Arcs

Theorem 2.2 (Dirichlet, [21, Lemma 2.1, p. 9])**.** *Let $\alpha \in \mathbb{R}$ and $Q > 1$. Then there exist integers a, q with $1 \leq q \leq Q$, $(a,q) = 1$, such that $\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}$.*

Proof. See [21, Lemma 2.1, p. 9]. □

Definition 2.3. Fix $0 < \delta < \frac{1}{5}$. For integers a, q with $1 \leq q \leq P^\delta$, $1 \leq a \leq q$ and $(a,q) = 1$, let

$$\mathfrak{M}(q,a) = \left\{\alpha \in \mathbb{R} : \ \left|\alpha - \frac{a}{q}\right| \leq P^{\delta - s}\right\},$$

as in [21, Section 2.1]. For P large, these intervals are pairwise disjoint, since $|a/q - a'/q'| \geq 1/(qq') \geq P^{-2\delta} > 2P^{\delta-s}$ for $a/q \neq a'/q'$, and all of them lie in $[0,1]$ except

$\mathfrak{M}(1,1) = [1 - P^{\delta-s}, 1 + P^{\delta-s}]$, since $1/q \geq P^{-\delta} > P^{\delta-s}$. We read the intervals modulo 1, that is, we move the part $(1, 1 + P^{\delta-s}]$ of $\mathfrak{M}(1,1)$ back by 1 and replace $\mathfrak{M}(1,1)$ by $[0, P^{\delta-s}] \cup [1 - P^{\delta-s}, 1]$. The set of major arcs is

$$\mathfrak{M} = \mathfrak{M}_\delta = \bigcup_{\substack{1 \leq q \leq P^\delta \\ 1 \leq a \leq q,\ (a,q)=1}} \mathfrak{M}(q,a) \ \subseteq \ [0,1],$$

and the minor arcs are the complement $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$.

2.4 The Minor Arcs

Theorem 2.4 (Weyl's inequality, Weyl [27]). *Let $s \geq 2$ and $\phi(x) = \lambda_s x^s + \lambda_{s-1} x^{s-1} + \cdots + \lambda_0$ with $\lambda_0, \ldots, \lambda_s \in \mathbb{R}$. Suppose there exist coprime integers a, q with $|\lambda_s - a/q| \leq q^{-2}$. Then for any $\varepsilon > 0$,*

$$\sum_{1 \leq x \leq P} e\big(\phi(x)\big) \ \ll_{s,\varepsilon} \ P^{1+\varepsilon}\Big(q^{-1} + P^{-1} + qP^{-s}\Big)^{2^{1-s}}.$$

Proof. See [21, Lemma 2.4, p. 11]. □

Lemma 2.5 (Hua's lemma, Hua [10]). *Let $s \geq 1$. For any integer j with $1 \leq j \leq s$ and any $\varepsilon > 0$,*

$$\int_0^1 \big|S(\alpha)\big|^{2^j} d\alpha \ \ll_{s,\varepsilon} \ P^{2^j - j + \varepsilon}.$$

Proof. See [10] and [21, Lemma 2.5, p. 12]. □

Dirichlet's theorem, Weyl's inequality and Hua's lemma give the following estimate.

Theorem 2.6 (Vaughan [21], Theorem 2.1, p. 14). *Let $s \geq 2$, $0 < \delta < \frac{1}{5}$, and suppose $k \geq 2^s + 1$. Then, for every $\varepsilon > 0$,*

$$\Big|\int_{\mathfrak{m}} S(\alpha)^k \, e(-N\alpha)\, d\alpha\Big| \ \ll \ P^{k - s - \delta 2^{1-s} + \varepsilon}.$$

Proof. See [21, Theorem 2.1, p. 14]. □

2.5 The Major Arcs

Define, for integers a, q with $1 \le a \le q$, the complete exponential sum $S(q,a)$ and the integral $V(\beta)$ by

$$S(q,a) = \sum_{r=1}^{q} e\Big(\frac{ar^s}{q}\Big), \qquad V(\beta) = \int_0^P e\big(\beta y^s\big)\, dy.$$

Lemma 2.7 (Vaughan [21], Lemma 2.7, p. 14)**.** *Let $a, q \in \mathbb{N}$ with $1 \le a \le q$ and $(a,q) = 1$, and, for $\alpha \in \mathbb{R}$, write $\beta = \alpha - \frac{a}{q}$. Then*

$$S(\alpha) \;-\; \frac{1}{q}\, S(q,a)\, V(\beta) \;\ll\; q \;+\; P^s\, |q\alpha - a|,$$

where the implied constant depends only on s. In particular, if $\alpha \in \mathfrak{M}(q,a)$, then the left-hand side is $\ll P^{2\delta}$.

Proof. See [21, Lemma 2.7 and the remark after it, p. 14]. □

Define

$$\mathfrak{S}_{s,k}(N,Q) = \sum_{\substack{1\le q\le Q\\ 1\le a\le q,\ (a,q)=1}} q^{-k} S(q,a)^k\, e(-Na/q), \quad \mathfrak{J}_{s,k}(N,Q) = \int_{-QP^{-s}}^{QP^{-s}} V(\beta)^k e(-N\beta)\, d\beta.$$

Lemma 2.8 (Vaughan [21], equations (2.13)–(2.15), p. 16)**.** *If $0 < \delta < \frac{1}{5}$, then there exists $u = u(s,\delta) > 0$, depending only on s and δ, such that*

$$\int_{\mathfrak{M}} S(\alpha)^k e(-N\alpha)\, d\alpha \;=\; \mathfrak{S}_{s,k}\big(N, P^\delta\big)\, \mathfrak{J}_{s,k}\big(N, P^\delta\big) \;+\; O\big(P^{k-s-u}\big).$$

Proof. See [21, equations (2.13)–(2.15), p. 16]. □

Lemma 2.9 (Vaughan [21], Lemma 2.4, p. 11, and p. 17)**.** *For $a, q \in \mathbb{N}$ with $1 \le a \le q$ and $(a,q) = 1$, we have $S(q,a) \;\ll\; q^{\,1-2^{1-s}+\varepsilon}$.*

Proof. See [21, p. 17]. □

Definition 2.10 (Singular series)**.** The singular series is

$$\mathfrak{S}_{s,k}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \big(q^{-1}S(q,a)\big)^k e(-Na/q).$$

By the last lemma, the q-th term of the series is $\ll q^{1-k2^{1-s}+k\varepsilon}$, so for $k \geq 2^s+1$ and $\varepsilon \leq 2^{-s}/k$ this term is $\ll q^{-1-2^{-s}}$, as in [21, equation (2.17), p. 17]. Hence the series converges absolutely and

$$\mathfrak{S}_{s,k}(N) - \mathfrak{S}_{s,k}(N,Q) \ \ll \ Q^{-2^{-s}}.$$

Lemma 2.11 (Vaughan [21], Lemma 2.8, p. 17)**.** *For $\beta \in \mathbb{R}$, we have $|V(\beta)| \ \ll \ P\,(1+|\beta|P^s)^{-1/s}$.*

Proof. See [21, Lemma 2.8, p. 17]. □

Definition 2.12 (Singular integral)**.** The singular integral is

$$\mathfrak{J}_{s,k}(N) \ = \ \int_{-\infty}^{\infty} V(\beta)^k\, e(-N\beta)\, d\beta.$$

By the bound on $V(\beta)$, for $k \geq s+1$ the integral converges absolutely, and

$$\mathfrak{J}_{s,k}(N) \ \ll \ P^{k-s}, \qquad \mathfrak{J}_{s,k}(N) - \mathfrak{J}_{s,k}(N,Q) \ \ll \ P^{k-s}\,Q^{-1/s}.$$

Theorem 2.13 (Vaughan [21], equations (2.13) and (2.21), pp. 16–18)**.** *Suppose $k \geq 2^s+1$. Then for any fixed $0 < \delta < \frac{1}{5}$ there exists $w = w(s,\delta) > 0$ such that*

$$\int_{\mathfrak{M}} S(\alpha)^k e(-N\alpha)\, d\alpha = \mathfrak{S}_{s,k}(N)\,\mathfrak{J}_{s,k}(N) \ + \ O\big(P^{k-s-w}\big).$$

Proposition 2.14 (Vaughan [21], Theorem 2.3, p. 19)**.** *Assume $k \geq s+1$. Then*

$$\mathfrak{J}_{s,k}(N) \ = \ \frac{\Gamma\big(1+\frac{1}{s}\big)^k}{\Gamma\big(\frac{k}{s}\big)}\, N^{\frac{k}{s}-1}\big(1+O(N^{-1/s})\big),$$

where Γ is the Gamma function.

Proof. See [21, Theorem 2.3, p. 19]. □

2.6 Lower Bound for $\mathfrak{S}_{s,k}(N)$

To conclude that the major arcs dominate, it suffices to show $1 \ll \mathfrak{S}_{s,k}(N) \ll 1$. The upper bound was proved above. For the lower bound, define

$$A(q,N) \;=\; \sum_{\substack{a=1\\(a,q)=1}}^{q} \big(q^{-1}S(q,a)\big)^k e\!\left(-\frac{Na}{q}\right), \qquad \sigma_p \;=\; \sum_{h=0}^{\infty} A(p^h,N),$$

where p denotes a prime.

Proposition 2.15 (Vaughan [21], Theorem 2.4, p. 20)**.** *Assume $s \geq 2$ and $k \geq 2^s + 1$. Then every series σ_p converges absolutely, there is $\eta_1 = \eta_1(s) > 0$ with $\big|\sigma_p - 1\big| \ll p^{-1-\eta_1}$, and*

$$\mathfrak{S}_{s,k}(N) = \prod_p \sigma_p,$$

the product being absolutely convergent. Moreover, there exists $C = C(s,k) > 0$ such that $\frac{1}{2} < \prod_{p>C} \sigma_p < \frac{3}{2}$.

Proof. See [21, Theorem 2.4, p. 20]. □

So it remains to bound σ_p from below, uniformly in N, for the finitely many primes $p \leq C$. For $q \geq 1$, let $M_N(q)$ be the number of solutions of $x_1^s + \cdots + x_k^s \equiv N \pmod q$ in $(\mathbb{Z}/q\mathbb{Z})^k$, and let $M_N^*(q)$ be the number of such solutions with $(x_1, q) = 1$.

Lemma 2.16 (Vaughan [21], Lemma 2.12, p. 21)**.** *For every natural number q, we have $\sum_{d|q} A(d,N) = q^{1-k} M_N(q)$. In particular,*

$$\sigma_p \;=\; \lim_{h\to\infty} p^{h(1-k)}\, M_N(p^h),$$

so σ_p is the p-adic density of solutions.

Proof. See [21, Lemma 2.12, p. 21]. □

Let $v_p(s)$ be the exponent of p in s, so that $p^{v_p(s)} \parallel s$, and let $\nu = v_p(s) + 1$ for $p > 2$ or $(p, v_p(s)) = (2,0)$, and $\nu = v_p(s) + 2$ for $p = 2$, $v_p(s) > 0$.

Lemma 2.17 (Vaughan [21], Lemma 2.13, p. 22)**.** *If $M_N^*(p^\nu) > 0$, then, for every $h \geq \nu$, one has $M_N(p^h) \geq p^{(h-\nu)(k-1)}$.*

Proof. See [21, Lemma 2.13, p. 22]. □

Lemma 2.18 (Vaughan [21], Lemma 2.15, p. 23)**.** *Suppose that*

$$k \;\geq\; \begin{cases} \dfrac{p}{p-1}\gcd\big(s, p^{v_p(s)}(p-1)\big), & \nu = v_p(s)+1, \\ 2^{v_p(s)+2}, & \nu = v_p(s)+2 \text{ and } s > 2, \\ 5, & p = s = 2. \end{cases}$$

Then $M_N^*(p^\nu) \geq 1$.

Proof. See [21, Lemma 2.15, p. 23]. □

Each of the three conditions of Lemma 2.18 follows from $k \geq 2^s + 1$. The first bound is at most $\frac{p}{p-1}s \leq 2s \leq 2^s + 1$. In the second case, $2^{v_p(s)}$ divides s and $s \geq 4$, so $2^{v_p(s)+2} \leq 4s \leq 2^s + 1$. The third bound is $5 = 2^2 + 1$. By the three lemmas, for $k \geq 2^s + 1$ and every $p \leq C$,

$$\sigma_p = \lim_{h\to\infty} p^{h(1-k)} M_N(p^h) \;\geq\; p^{-\nu(k-1)} \;>\; 0,$$

and hence

$$\mathfrak{S}_{s,k}(N) = \Big(\prod_{p\leq C}\sigma_p\Big)\Big(\prod_{p>C}\sigma_p\Big) \;\geq\; \Big(\prod_{p\leq C} p^{-\nu(k-1)}\Big)\cdot\frac{1}{2} \;\gg_{s,k}\; 1.$$

Proposition 2.19 (Vaughan [21], Theorem 2.5, p. 24, and equation (2.19), p. 17)**.** *If* $k \geq 2^s + 1$*, then* $1 \ll \mathfrak{S}_{s,k}(N) \ll 1$*, where the implied constants depend only on* s *and* k*.*

2.7 The Asymptotic Formula

Combining the minor-arc bound, the major-arc theorem, and the bounds for the singular series, we obtain the asymptotic formula. We fix δ to be $\frac{1}{10}$. The exponents in Theorems 2.6 and 2.13 depend on δ, and with δ fixed they depend only on s, so the two error terms combine into one error term with an exponent $w = w(s)$. Any fixed δ with $0 < \delta < \frac{1}{5}$ would do.

Theorem 2.20 (Vaughan [21], Theorem 2.6, p. 24)**.** *If* $k \geq 2^s + 1$*, then there exists* $w = w(s) > 0$ *such that*

$$R_{s,k}(N) = \mathfrak{S}_{s,k}(N)\,\frac{\Gamma(1+\frac{1}{s})^k}{\Gamma(\frac{k}{s})}\,N^{\frac{k}{s}-1} + O\big(N^{\frac{k}{s}-1-w}\big),$$

where the implied constant depends only on k *and* s*.*

In particular, $R_{s,k}(N) > 0$ for N large, so $G(s) \le 2^s + 1$. Vinogradov's method gives $G(s) \le 32(s \ln s)^2$ [23], and its later refinements give $G(s) \le 6s \ln s + 3s \ln 6 + 4s$ and $G(s) \le s(3 \ln s + 11)$ [24]; see [22, Section 3, Table 1]. The best known bound is, for $s \ge 14$,

$$G(s) \le \Big\lceil s\big(\ln s + 4.20032\big)\Big\rceil,$$

due to Brüdern and Wooley [4].

Chapter 3

The Hilbert-Kamke Problem in Integers

This chapter reviews the classical Hilbert-Kamke problem over the integers. All results in this chapter can be found in the book of Arkhipov, Chubarikov and Karatsuba [3], and we refer to the book for the proofs.

3.1 The Asymptotic Formula

The solubility of the Hilbert-Kamke system for large $N_1, \dots, N_n$ depends on three estimates: positive lower bounds independent of P and $N_1, \dots, N_n$ for the singular series and for the normalized singular integral, and an estimate of the minor arcs. The last two are established in [3], and this thesis is concerned only with the singular series. Let $n \geq 3$, and let $k, N_1, \dots, N_n, P$ be natural numbers. Let $r(\boldsymbol{N}, P)$ denote the number of solutions in natural numbers $x_1, \dots, x_k \leq P$ of the system of equations

$$\sum_{i=1}^{k} x_i^s = N_s, \quad s = 1, \dots, n.$$

Here $\boldsymbol{N} = (N_1, \dots, N_n)$. In [3], the variables are natural numbers, as in this thesis.

The formula below is proved by the circle method as in Chapter 2; see [3, Chapter 3]. In place of one variable, we integrate over $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$, and the counting function is

written as

$$r(\boldsymbol{N},P)=\int_{[0,1]^n} S(\boldsymbol{\beta})^k\, e\big(-(\beta_1N_1+\cdots+\beta_nN_n)\big)\,d\boldsymbol{\beta},\quad S(\boldsymbol{\beta})=\sum_{x=1}^{P} e(\beta_1x+\cdots+\beta_nx^n),$$

where $e(\alpha)=e^{2\pi i\alpha}$ as in Chapter 2. The cube $[0,1]^n$ is divided into major and minor arcs. The major arcs give the main term $\sigma_{\mathbb{Z}}\,\tau_{\mathbb{Z}}P^{\,k-\frac{1}{2}n(n+1)}$, where the singular series $\sigma_{\mathbb{Z}}$ is a sum over the points $(a_1/q_1,\dots,a_n/q_n)$ of the cube and is determined by the solutions of the system modulo every integer, and the normalized singular integral $\tau_{\mathbb{Z}}$ is determined by the real solutions of the system. The minor arcs give the error term.

Theorem 3.1 (Arkhipov, Chubarikov and Karatsuba, [3, Theorem 3.7, p. 114])**.** *Let $n\ge 3$, $k\ge n^2(4\ln n+2\ln\ln n+9)$ and $k\le P^{0.1}$. Then*

$$r(\boldsymbol{N},P)=\sigma_{\mathbb{Z}}\tau_{\mathbb{Z}}P^{k-\frac{1}{2}n(n+1)}+\varrho\, n^{30n^3}P^{k-\frac{1}{2}n(n+1)-(30(2+\ln n))^{-1}}.$$

Here ϱ is a real number with $|\varrho|\le 1$, and $\sigma_{\mathbb{Z}}$ and $\tau_{\mathbb{Z}}$ are non-negative numbers. The value of $\sigma_{\mathbb{Z}}$ is equal to the sum of the singular series in the Hilbert-Kamke problem and the value of $\tau_{\mathbb{Z}}$ is equal to the value of the normalized singular integral in the Hilbert-Kamke problem. Namely,

$$\sigma_{\mathbb{Z}}=\sum_{q_1=1}^{\infty}\cdots\sum_{q_n=1}^{\infty}\sum_{\substack{1\le a_1\le q_1\\(a_1,q_1)=1}}\cdots\sum_{\substack{1\le a_n\le q_n\\(a_n,q_n)=1}} q^{-k}\,S(\boldsymbol{q},\boldsymbol{a})^k\,e\Big(-\frac{a_1N_1}{q_1}-\cdots-\frac{a_nN_n}{q_n}\Big),$$

$$\tau_{\mathbb{Z}}=\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty} V(\boldsymbol{z})^k\,e\Big(-\frac{z_1N_1}{P}-\cdots-\frac{z_nN_n}{P^n}\Big)\,dz_1\dots dz_n,$$

where $q=q_1\cdots q_n$, $\boldsymbol{q}=(q_1,\dots,q_n)$, $\boldsymbol{a}=(a_1,\dots,a_n)$, $\boldsymbol{z}=(z_1,\dots,z_n)$,

$$S(\boldsymbol{q},\boldsymbol{a})=\sum_{x=1}^{q} e\left(\frac{a_1x}{q_1}+\cdots+\frac{a_nx^n}{q_n}\right),\qquad V(\boldsymbol{z})=\int_0^1 e(z_1x+\cdots+z_nx^n)\,dx.$$

The singular series $\sigma_{\mathbb{Z}}$ converges absolutely for $k>\frac{1}{2}n(n+1)+2$, and the singular integral $\tau_{\mathbb{Z}}$ converges absolutely for $k>\frac{1}{2}n(n+1)+1$.

Proof. See [3, Theorem 3.7, p. 114]. □

The asymptotic formula gives a solution of the system for large P if $\sigma_{\mathbb{Z}}$ and $\tau_{\mathbb{Z}}$ are bounded below by positive constants independent of P and $N_1, \ldots, N_n$. The positivity of $\sigma_{\mathbb{Z}}$ and $\tau_{\mathbb{Z}}$ is not enough, since $\sigma_{\mathbb{Z}}$ depends on $N_1, \ldots, N_n$ and $\tau_{\mathbb{Z}}$ depends on $N_1, \ldots, N_n$ and P, and the lower bounds must not depend on them. By Lemma 3.2 below, $\sigma_{\mathbb{Z}}$ is the product over the primes p of local densities, the local density at p being the limit of the normalized number of solutions of the system modulo the powers of p. If the system has no solution modulo some power of p, then it has no solution modulo the higher powers of p either, the local density at p is zero, and so is $\sigma_{\mathbb{Z}}$. The system itself then has no solutions at all. However, the existence of local solutions only gives a positive value of the local density; it does not give a lower bound independent of $N_1, \ldots, N_n$. Theorem 3.9 below gives such a lower bound for $\sigma_{\mathbb{Z}}$ for k large, a constant depending only on n, by a lower bound for every local density and a lower bound for the product over the large primes. Theorem 8.2(1) of [3, p. 343] shows that for $k < 2^n - 1$ there are $N_1, \ldots, N_n$ satisfying the arithmetic condition (3.1) below for which $\sigma_{\mathbb{Z}} = 0$. The estimate of the minor arcs is given by Wooley (Remark 4.10), and the lower bound for $\tau_{\mathbb{Z}}$ follows from the growth condition (Lemma 3.10). So the remaining problem for the existence of solutions is the lower bound for the singular series $\sigma_{\mathbb{Z}}$.

3.2 The Singular Series

For a natural number d and $x_1, \ldots, x_k$ running over a complete residue system modulo d, we define $W(d, k)$ as the number of solutions of the system of congruences

$$x_1^s + \cdots + x_k^s \equiv N_s \pmod{d}, \quad s = 1, \ldots, n.$$

We let p denote a prime number.

Lemma 3.2 (Arkhipov, Chubarikov and Karatsuba, [3, Lemmas 8.1 and 8.2, pp. 317–319])**.** *Let $n \geq 3$, let $u \in \mathbb{N}$ and $M = u!$, and let k be an integer such that*

$$k > \frac{n(n+1)}{2} + 2.$$

Then the singular series $\sigma_{\mathbb{Z}}$ satisfies

$$\sigma_{\mathbb{Z}} = \lim_{u \to \infty} W(M, k)\, M^{n-k}.$$

Moreover, if we let

$$\sigma_p = \lim_{h \to \infty} W\big(p^h, k\big)\, p^{h(n-k)},$$

then we have

$$\sigma_{\mathbb{Z}} = \prod_{p} \sigma_p,$$

where the product runs over all primes p.

Proof. See [3, Lemmas 8.1 and 8.2, pp. 317–319]. □

3.3 An Arithmetic Condition

Lemma 3.3 (Arkhipov, Chubarikov and Karatsuba, [3, p. 320])**.** *Let $n \geq 1$. For any integer x, the system*

$$\sum_{r=1}^{n} t_r r^s = x^s, \quad s = 1, \ldots, n,$$

has an integer solution of the form

$$t_r = \binom{x}{r}\binom{n-x}{n-r}, \quad r = 1, \ldots, n,$$

where $\binom{x}{a}$ is defined for any natural number a by

$$\binom{x}{a} = \frac{x(x-1)\cdots(x-a+1)}{a!},$$

and $\binom{x}{0} = 1$.

Proof. See [3, p. 320]. □

Let $\Gamma_n(\mathbb{Z}) \subseteq \mathbb{Z}^n$ be the set of all $\mathbb{Z}$-linear combinations of the vectors $(x, x^2, \ldots, x^n)$, $x \in \mathbb{Z}$. By Lemma 3.3, every vector $(x, x^2, \ldots, x^n)$ is a $\mathbb{Z}$-linear combination of the n vectors $(r, r^2, \ldots, r^n)$, $1 \leq r \leq n$, and these n vectors lie in $\Gamma_n(\mathbb{Z})$, so $\Gamma_n(\mathbb{Z})$ is the set of $\mathbb{Z}$-linear combinations of these n vectors. If the Hilbert-Kamke system has a solution in integers, then $(N_1, \ldots, N_n) = \sum_{i=1}^{k}(x_i, x_i^2, \ldots, x_i^n)$ lies in $\Gamma_n(\mathbb{Z})$. From now on, we assume that $N_1, \ldots, N_n$ $(n \geq 3)$ satisfy the following condition. The system of linear equations

$$\sum_{r=1}^{n} t_r r^s = N_s, \quad s = 1, \ldots, n \tag{3.1}$$

has a solution in integers $t_1, \ldots, t_n$. This condition says that $(N_1, \ldots, N_n)$ is a $\mathbb{Z}$-linear combination of the n vectors $(r, r^2, \ldots, r^n)$, $1 \le r \le n$, that is, that $(N_1, \ldots, N_n) \in \Gamma_n(\mathbb{Z})$. We call this condition the arithmetic condition. It is condition (8.5) of [3, p. 320], and, by the above, it is necessary for the solubility of the system. Chapter 5 replaces $\Gamma_n(\mathbb{Z})$ by the set $\Gamma_n(\mathcal{O}_K)$ of $\mathbb{Z}$-linear combinations of the vectors $(x, x^2, \ldots, x^n)$ with $x \in \mathcal{O}_K$, and condition (3.1) by Condition (M) of Definition 5.3.

Recall that the goal is a positive lower bound for $\sigma_{\mathbb{Z}}$ independent of $N_1, \ldots, N_n$. Hence it suffices to find lower bounds $W(p^h, k) \ge c_p\, p^{h(k-n)}$ with constants c_p independent of h and of $N_1, \ldots, N_n$, such that the product of c_p over all large enough p is positive. We divide the problem into the two cases $p \le n$ and $p > n$. Section 3.6 gives a sharper bound for $p \ge 9n^2$.

3.4 Result for $p \le n$

Lemma 3.4 (Arkhipov, Chubarikov and Karatsuba, [3, Lemma 8.3, p. 321])**.** *Let $n \ge 3$, and suppose that $N_1, \ldots, N_n$ satisfy condition* (3.1)*. Suppose that $p \le n$ and $k \ge n^2 2^{2n-1} = k_1$. Then, for every natural number h,*

$$W(p^h, k) \ge c_*^{\mathbb{Q}}\, p^{h(k-n)} > 0,$$

where $c_*^{\mathbb{Q}} = p^{(2\varkappa+2\delta+1)(n-k_1)}$, $\varkappa$ is the integer determined by the condition

$$p^{\varkappa} \le n < p^{\varkappa+1},$$

and δ is the exponent of p in the factorization of $(n-1)!$.

Proof. See [3, Lemma 8.3, p. 321]. □

3.5 Result for $p > n$

Let $n \ge 3$, and let p be a prime number with $p > n$. Let T_1 be the number of solutions of the system of congruences

$$x_1^s + \cdots + x_k^s \equiv N_s \pmod{p}, \qquad s = 1, \ldots, n, \qquad 1 \le x_1, \ldots, x_k \le p,$$

so that $T_1 = W(p, k)$. In [3], the next two lemmas are stated for exponents $r_1 < \cdots < r_l = n$; we state them for the exponents $1, \ldots, n$.

Lemma 3.5 (Arkhipov, Chubarikov and Karatsuba, [3, Lemma 8.5, p. 333], due to Linnik)**.** *Let $n \geq 3$, $p > n$ and $k \geq 1$. Then T_1 satisfies the asymptotic formula*

$$T_1 = p^{k-n} + \varrho\,(np^{1/2})^k, \qquad |\varrho| \leq 1.$$

Moreover, $T_1 \geq 1$ if $p \geq 9n^2$ and $k \geq 4n \ln n$.

Proof. See [3, Lemma 8.5, p. 333]. □

Lemma 3.6 (Arkhipov, Chubarikov and Karatsuba, [3, Lemma 8.6, p. 333])**.** *Let $n \geq 3$. Let $n < p \leq 9n^2$, and let $k \geq \lfloor 32n^2 \ln n \rfloor$. Then $T_1 \geq 1$.*

Proof. See [3, Lemma 8.6, p. 333]. □

From now on, we write

$$k_2 = \lfloor 32n^2 \ln n \rfloor + n.$$

The n additional variables are used in the next lemma, whose proof needs a solution modulo p with $x_i \equiv i \pmod p$ for $1 \leq i \leq n$, which is obtained from Lemmas 3.5 and 3.6 applied to the remaining $k - n$ variables.

Lemma 3.7 (Arkhipov, Chubarikov and Karatsuba, [3, Lemma 8.7, p. 335])**.** *Let $n \geq 3$. Suppose that $p > n$, $k \geq k_2 = \lfloor 32n^2 \ln n \rfloor + n$, and h is a natural number. Then*

$$W(p^h, k) \geq p^{n-k_2} p^{h(k-n)}.$$

Proof. See [3, Lemma 8.7, p. 335]. □

3.6 Result for $p \geq 9n^2$

Lemma 3.8 (Arkhipov, Chubarikov and Karatsuba, [3, Lemma 8.8, p. 335])**.** *Let $n \geq 3$. The following estimate holds for $p \geq 9n^2$, $k \geq 6n^2$ and every natural number h:*

$$W(p^h, k) \geq p^{h(k-n)}(1 - p^{-3}).$$

Proof. See [3, Lemma 8.8, p. 335]. □

Theorem 3.9 (Arkhipov, Chubarikov and Karatsuba, [3, Theorem 8.1, p. 337]). *Let $n \geq 3$ and $k \geq \max(k_1, k_2)$, where $k_1 = n^2 2^{2n-1}$ and $k_2 = \lfloor 32n^2 \ln n \rfloor + n$. Then, under condition (3.1),*

$$\sigma_{\mathbb{Z}} \geq n^{-20n^4 2^n}.$$

Proof. See [3, Theorem 8.1, p. 337]. □

For $n \geq 4$, one has $k_1 \geq k_2$, so that the condition $k \geq \max(k_1, k_2)$ is $k \geq k_1$.

3.7 Solubility of the System

Theorems 3.1 and 3.9 together give the solubility of the system for large P. This needs a positive lower bound for $\tau_{\mathbb{Z}}$ independent of P and $N_1, \ldots, N_n$. The lower bound for $\tau_{\mathbb{Z}}$ is determined by the real system

$$x_1^s + \cdots + x_k^s = N_s P^{-s}, \qquad s = 1, \ldots, n, \qquad 0 \leq x_1, \ldots, x_k \leq 1. \tag{3.2}$$

Following [3, p. 346], for a point $(x_1, \ldots, x_k) \in [0,1]^k$ and n of its coordinates $z_1, \ldots, z_n$, let $z_0 = 0$ and $z_{n+1} = 1$, and form $\min_{0 \leq i < j \leq n+1} |z_i - z_j|$. The largest value of this minimum over all choices of n coordinates is the *characteristic* of the point. Let $\lambda = \lambda(N_1, \ldots, N_n, P)$ be the largest characteristic of a solution of (3.2), and $\lambda = 0$ if (3.2) has no solution.

Lemma 3.10 (Arkhipov, Chubarikov and Karatsuba, [3, Theorem 8.3, p. 352]). *Let $n \geq 3$ and $k > \frac{1}{2}n(n+1) + 1$. Then*

$$2^{2n(n-k)}\, k^{n-k}\, n^{-k-n}\, \lambda^{n(k-n)} \;\leq\; \tau_{\mathbb{Z}} \;\leq\; 2^{2n^2}\, k^{2n}\, n^{k-2n}\, \lambda^{k-3n-n^2}.$$

In particular, $\tau_{\mathbb{Z}} > 0$ if and only if $\lambda > 0$, and, for every $\lambda_0 > 0$ and all $N_1, \ldots, N_n, P$ with $\lambda(N_1, \ldots, N_n, P) \geq \lambda_0$,

$$\tau_{\mathbb{Z}} \;\geq\; 2^{2n(n-k)}\, k^{n-k}\, n^{-k-n}\, \lambda_0^{n(k-n)}.$$

Proof. See [3, Theorem 8.3, p. 352]. □

Fix $\lambda_0 > 0$. The condition $\lambda(N_1, \ldots, N_n, P) \geq \lambda_0$ depends on $N_1, \ldots, N_n$ only through the quotients $N_s P^{-s}$, and by Lemma 3.10 it gives a positive lower bound for $\tau_{\mathbb{Z}}$ that depends only on n, k and λ_0. This is the growth condition of Section 1.2.

Theorem 3.11 (Arkhipov, Chubarikov and Karatsuba, [3, Theorem 3.7, Theorem 8.1 and Remark 8.1, pp. 114, 337 and 353])**.** *Let $n \geq 3$, let $k \geq \max\big(n^2(4\ln n + 2\ln\ln n + 9),\, k_1, k_2\big)$, let $\lambda_0 > 0$, and suppose that $N_1, \ldots, N_n$ satisfy condition* (3.1) *and $\lambda(N_1, \ldots, N_n, P) \geq \lambda_0$. Then there is $P_0 = P_0(n, k, \lambda_0)$ such that for every $P \geq P_0$ the system $x_1^s + \cdots + x_k^s = N_s$, $s = 1, \ldots, n$, has a solution with $1 \leq x_i \leq P$.*

Proof. By Theorem 3.9 and Lemma 3.10, the main term in Theorem 3.1 satisfies

$$\sigma_{\mathbb{Z}}\, \tau_{\mathbb{Z}}\, P^{\,k-\frac{1}{2}n(n+1)} \;\geq\; n^{-20n^4 2^n}\, 2^{2n(n-k)}\, k^{\,n-k}\, n^{-k-n}\, \lambda_0^{\,n(k-n)}\, P^{\,k-\frac{1}{2}n(n+1)},$$

while the error term is at most $n^{30n^3} P^{\,k-\frac{1}{2}n(n+1)-(30(2+\ln n))^{-1}}$. The quotient of the two bounds tends to infinity with P, so there is $P_0 = P_0(n, k, \lambda_0) \geq k^{10}$ such that for $P \geq P_0$ the main term exceeds the error term and $r(\boldsymbol{N}, P) > 0$. □

Thus the arithmetic part of the problem is the singular series, and we study its analogue over number fields in the rest of the thesis.

Chapter 4

Number Fields

Chapter 2 stated the circle method of Hardy and Littlewood for Waring's problem, and Chapter 3, the asymptotic formula for the Hilbert-Kamke system over $\mathbb{Q}$. Siegel [19, 20] introduced the circle method for the ring of integers $\mathcal{O}_K$ of a number field K and applied it to Waring's problem over K. We follow Siegel's papers [19, 20] and the book of Wang [25], which are written for a single equation $x_1^s + \cdots + x_k^s = N$ over $\mathcal{O}_K$, and extend the method to the Hilbert-Kamke system with $N_1, \ldots, N_n \in \mathcal{O}_K$ and $x_1, \ldots, x_k \in \mathcal{O}_K$,

$$x_1^s + \cdots + x_k^s = N_s, \qquad s = 1, \ldots, n.$$

Here the exponential sum has n coefficients $\alpha_1, \ldots, \alpha_n$, so the Farey dissection is made for the n coefficients together, and the singular series is a sum over n-tuples of fractions whose local factors count the solutions of a system of n congruences.

The main results are Theorem 4.20, the absolute convergence of the singular series σ_K for $k > n(n+1)$ (from now on, we write σ for σ_K), Theorem 4.21, the asymptotic formula for the integral over the major arcs, Lemma 4.22 and Theorem 4.24, the product formula $\sigma = \prod_\wp \sigma_\wp$ with $\sigma_\wp$ the density of solutions of the system modulo the powers of $\wp$, and Theorem 4.30, which reduces the lower bound for σ to the non-singular solubility of the system modulo finitely many prime ideal powers. The lower bounds themselves are proved in Chapters 5 and 6, one prime ideal at a time.

4.1 Number Fields and Rings of Integers

This section fixes the notation and recalls the facts about algebraic number fields used in this thesis. The material is standard, and proofs can be found in [13] and [15].

A *number field* K is a finite extension of $\mathbb{Q}$. For the rest of the thesis, we assume that $[K : \mathbb{Q}] = m$. Then K is a vector space of dimension m over $\mathbb{Q}$.

The *ring of integers* $\mathcal{O}_K$ of K is the set of elements of K that are roots of monic polynomials with coefficients in $\mathbb{Z}$,

$$\mathcal{O}_K = \{\alpha \in K \mid f(\alpha) = 0 \text{ for some monic } f(x) \in \mathbb{Z}[x]\}.$$

It is a subring of K, and it is the analogue of $\mathbb{Z}$ in K. The additive group of $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank m, so $\mathcal{O}_K$ has an *integral basis* $\{\omega_1, \ldots, \omega_m\}$, that is, a basis over $\mathbb{Z}$. For every $\alpha \in \mathcal{O}_K$, there are unique integers $c_1, \ldots, c_m$ with

$$\alpha = c_1\omega_1 + \cdots + c_m\omega_m.$$

4.1.1 Real and Complex Embeddings

Let $\iota_1, \ldots, \iota_m$ be the field homomorphisms (embeddings) of K into $\mathbb{C}$. For $\alpha \in K$, we write $\alpha^{(i)} = \iota_i(\alpha)$ for $1 \leq i \leq m$. An embedding ι_i is *real* if $\iota_i(K) \subseteq \mathbb{R}$, and *complex* otherwise. The complex embeddings come in pairs of complex conjugate embeddings. We number the embeddings so that $\iota_1, \ldots, \iota_{r_1}$ are the real ones and, for $\gamma \in K$ and $1 \leq j \leq r_2$,

$$\iota_{r_1+r_2+j}(\gamma) = \overline{\iota_{r_1+j}(\gamma)},$$

where the bar denotes complex conjugation. Here r_1 is the number of real embeddings, r_2 is the number of pairs of complex embeddings, and $m = r_1 + 2r_2$.

4.1.2 Norm and Trace

The *norm* and the *trace* of $\alpha \in K$ are

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{m} \alpha^{(i)}, \qquad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{m} \alpha^{(i)}.$$

Both are rational numbers, and they are integers for $\alpha \in \mathcal{O}_K$. The norm is multiplicative and the trace is additive: for $\alpha, \beta \in K$,

$$N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta), \qquad \mathrm{Tr}_{K/\mathbb{Q}}(\alpha + \beta) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) + \mathrm{Tr}_{K/\mathbb{Q}}(\beta).$$

For a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the *norm* of $\mathfrak{a}$ is the number of elements of the quotient ring $\mathcal{O}_K/\mathfrak{a}$,

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|.$$

It is a positive integer, it is multiplicative, $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$, and, for a non-zero $\alpha \in \mathcal{O}_K$, one has $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$ [15, Chapter 3, Theorem 22].

4.1.3 Discriminant and Different

The *discriminant* of K is

$$\Delta_K = \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j)\right)_{1\le i,j\le m},$$

where $\{\omega_1,\dots,\omega_m\}$ is an integral basis. It is a non-zero integer, and it does not depend on the choice of the integral basis.

A *fractional ideal* of K is an $\mathcal{O}_K$-submodule of K of the form $d^{-1}\mathfrak{a}$, where $\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_K$ and $d\in\mathcal{O}_K$ is non-zero. The *inverse* of a non-zero fractional ideal $\mathfrak{a}$ is

$$\mathfrak{a}^{-1} = \{x\in K \mid x\mathfrak{a}\subseteq\mathcal{O}_K\},$$

and it is again a fractional ideal. The bilinear form $(x,y)\mapsto\mathrm{Tr}_{K/\mathbb{Q}}(xy)$ on K is non-degenerate, and the set

$$\mathfrak{D}_{K/\mathbb{Q}}^{-1} = \{\alpha\in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\mathcal{O}_K)\subseteq\mathbb{Z}\}$$

is a fractional ideal, the *inverse different* of K. Here and throughout, for a subset $M\subseteq K$, we write $\mathrm{Tr}_{K/\mathbb{Q}}(M)=\{\mathrm{Tr}_{K/\mathbb{Q}}(x)\mid x\in M\}$, so $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\mathcal{O}_K)\subseteq\mathbb{Z}$ means that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\mu)\in\mathbb{Z}$ for every $\mu\in\mathcal{O}_K$. Since $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K)\subseteq\mathbb{Z}$, we have $\mathcal{O}_K\subseteq\mathfrak{D}_{K/\mathbb{Q}}^{-1}$. The *different* of K is the inverse of this fractional ideal,

$$\mathfrak{D}_{K/\mathbb{Q}} = (\mathfrak{D}_{K/\mathbb{Q}}^{-1})^{-1},$$

and $\mathcal{O}_K\subseteq\mathfrak{D}_{K/\mathbb{Q}}^{-1}$ gives $\mathfrak{D}_{K/\mathbb{Q}}\subseteq\mathcal{O}_K$, so the different is an ideal of $\mathcal{O}_K$, and

$$|\Delta_K| = N(\mathfrak{D}_{K/\mathbb{Q}})$$

[13, Chapter III, Section 1]. From now on, we write $\mathfrak{D}$ for $\mathfrak{D}_{K/\mathbb{Q}}$ and D for Δ_K.

4.2 The Setup of the Circle Method

Throughout the remainder of this chapter, K is a number field of degree $m=r_1+2r_2$ with ring of integers $\mathcal{O}_K$, different $\mathfrak{D}$ and discriminant $D=\Delta_K$. The number $n\ge 2$ is the highest exponent of the Hilbert-Kamke system, k is the number of variables, and $N_1,\dots,N_n\in\mathcal{O}_K$ are the given numbers in the system. (Chapters 3, 5 and 6 assume $n\ge 3$. The results of this chapter hold for every $n\ge 2$.) Constants implied by O and $\ll$ depend

at most on K, n, k and the parameter ε introduced below. They never depend on P, on ideals, or on the N_s.

The setup below is Siegel's generalized circle method [19, 20], in the form given by Wang [25, Chapter 5, pp. 58–70]. The space $K_{\mathbb{R}}$, the character E, the dual basis, the set $\mathcal{P}(P)$ and the Farey dissection appear in Wang's book. Since the exponential sum has n coefficients, the dissection is made on the torus $\mathbb{T} = (K_{\mathbb{R}}/\mathfrak{D}^{-1})^n$, and its basic domains are boxes Ω whose side length in the s-th coordinate is $2c_0T'P^{-s}$, where T' is a function of P defined in Section 4.2.4 that tends to infinity with P. The box is the same for every rational point, so the integral over the major arcs factors into a sum over the rational points and a single integral over Ω. The sum gives a partial sum of the singular series, and the integral gives the singular integral truncated to a box that expands to $K_{\mathbb{R}}^n$ as $P \to \infty$ (Section 4.3).

4.2.1 The Space $K_{\mathbb{R}}$ and the Character E

Let $\iota_1, \dots, \iota_{r_1}$ be the real embeddings of K and $\iota_{r_1+1}, \dots, \iota_{r_1+r_2}$ representatives of the pairs of complex embeddings, ordered so that $\iota_{r_1+r_2+j} = \overline{\iota_{r_1+j}}$ for $1 \le j \le r_2$. Define

$$K_{\mathbb{R}} = \big\{\xi = (\xi^{(1)}, \dots, \xi^{(m)}) \in \mathbb{C}^m \;\big|\; \xi^{(i)} \in \mathbb{R}\ (1 \le i \le r_1), \quad \xi^{(i+r_2)} = \overline{\xi^{(i)}}\ (r_1 < i \le r_1 + r_2)\big\},$$

an $\mathbb{R}$-algebra under componentwise addition and multiplication. The embeddings give a ring embedding $K \hookrightarrow K_{\mathbb{R}}$, $\gamma \mapsto (\gamma^{(1)}, \dots, \gamma^{(m)})$, and we identify K with its image. $\mathbb{R}$ embeds diagonally, and elements of K occurring in products or in the argument of E are taken via this embedding. Thus $\gamma\xi$, for $\gamma \in K$ and $\xi \in K_{\mathbb{R}}$, has components $\iota_i(\gamma)\xi^{(i)}$. Set

$$\operatorname{Tr}(\xi) = \sum_{i=1}^{m} \xi^{(i)}, \qquad E(\xi) = e\big(\operatorname{Tr}(\xi)\big), \qquad e(x) = e^{2\pi i x}.$$

The conjugation condition on $K_{\mathbb{R}}$ makes Tr real-valued. The map Tr is $\mathbb{R}$-linear and restricts to $\operatorname{Tr}_{K/\mathbb{Q}}$ on K, which justifies the notation. The function E is an additive character of $K_{\mathbb{R}}$, that is, $E(\xi + \zeta) = E(\xi)E(\zeta)$ and $|E(\xi)| = 1$ for all $\xi, \zeta \in K_{\mathbb{R}}$. For $\xi \in K_{\mathbb{R}}$, write $\|\xi\| = \max_{1 \le i \le m} |\xi^{(i)}|$.

Under the identification above, every fractional ideal $\mathfrak{l}$ of K is a lattice in the m-dimensional real vector space $K_{\mathbb{R}}$, that is, a discrete subgroup that contains an $\mathbb{R}$-basis of $K_{\mathbb{R}}$. Fix an integral basis $\{\omega_1, \dots, \omega_m\}$ of $\mathcal{O}_K$. Then $\mathcal{O}_K$ is the $\mathbb{Z}$-span of $\omega_1, \dots, \omega_m$, and

these form an $\mathbb{R}$-basis of $K_{\mathbb{R}} \subset \mathbb{C}^m$ because $\big(\det(\omega_j^{(i)})_{i,j}\big)^2 = D \neq 0$. An integral ideal $\mathfrak{a}$ satisfies $N(\mathfrak{a})\mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}_K$ with index $[\mathcal{O}_K : \mathfrak{a}] = N(\mathfrak{a})$ [15, Chapter 3]. As a subgroup of the free $\mathbb{Z}$-module $\mathcal{O}_K$, it is free of rank $\leq m$, and since it contains the lattice $N(\mathfrak{a})\mathcal{O}_K$, any $\mathbb{Z}$-basis of $\mathfrak{a}$ consists of m vectors spanning $K_{\mathbb{R}}$ over $\mathbb{R}$. A general fractional ideal satisfies $\psi\mathfrak{l} \subseteq \mathcal{O}_K$ for some $\psi \in \mathcal{O}_K \setminus \{0\}$, and multiplication by $\psi^{-1} \in K_{\mathbb{R}}^{\times}$ (all $\psi^{(i)}$ are non-zero) is an invertible $\mathbb{R}$-linear map of $K_{\mathbb{R}}$, so $\mathfrak{l} = \psi^{-1}(\psi\mathfrak{l})$ is again a lattice. Throughout, quotients such as $K_{\mathbb{R}}/\mathfrak{D}^{-1}$ and covolumes of fractional ideals refer to these embedded lattices.

Let $\{\rho_1, \ldots, \rho_m\} \subset K$ be the dual basis with respect to the trace, $\mathrm{Tr}(\rho_i\omega_j) = \delta_{ij}$. Then $\{\rho_1, \ldots, \rho_m\}$ is a $\mathbb{Z}$-basis of $\mathfrak{D}^{-1}$ (Lemma 4.5(i) below). Define

$$U_m = \left\{ \sum_{i=1}^{m} x_i\rho_i \;\middle|\; x_i \in [0,1) \right\} \subset K_{\mathbb{R}},$$

where each ρ_i is regarded as an element of $K_{\mathbb{R}}$ via the embedding $K \hookrightarrow K_{\mathbb{R}}$. The set U_m is a fundamental domain for $K_{\mathbb{R}}/\mathfrak{D}^{-1}$ (the ρ_i, a $\mathbb{Z}$-basis of a lattice, form an $\mathbb{R}$-basis of $K_{\mathbb{R}}$).

Two Haar measures on $K_{\mathbb{R}}$ will be used. For a variable $\alpha \in K_{\mathbb{R}}$, let $x_1, \ldots, x_m$ be its coordinates in the dual basis, $\alpha = \sum_i x_i\rho_i$. The Lebesgue measure $dx = dx_1 \cdots dx_m$ in these coordinates is the measure of [25, Chapter 5], and we write it dx as there. The letters $x_1, \ldots, x_m$ always denote the dual-basis coordinates of the variable of integration, whatever the letter for that variable, so that

$$\int_{U_m} f(\alpha)\, dx = \int_{[0,1)^m} f\Big(\sum_{i=1}^{m} x_i\rho_i\Big)\, dx_1 \cdots dx_m.$$

This measure gives U_m measure 1, and so induces the Haar measure of total mass 1 on the torus $K_{\mathbb{R}}/\mathfrak{D}^{-1}$. It makes the characters $\alpha \mapsto E(\nu\alpha)$, $\nu \in \mathcal{O}_K$, orthonormal on U_m (Lemma 4.3 below), and it is the measure in all integrals over U_m, over the torus $\mathbb{T} = (K_{\mathbb{R}}/\mathfrak{D}^{-1})^n$ and over subsets of these. On $K_{\mathbb{R}}^n$, we use the product measure, written $d\boldsymbol{x}$: for a variable $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in K_{\mathbb{R}}^n$ with $\alpha_s = \sum_i x_{s,i}\rho_i$, we write $d\boldsymbol{x} = \prod_{s=1}^{n}\prod_{i=1}^{m} dx_{s,i}$. The other measure, $d\xi = du_1 \cdots du_m$, given by the integral-basis coordinates $\xi = \sum_i u_i\omega_i$, normalizes the covolume of $\mathcal{O}_K$ to 1. Here the *covolume* of a lattice is the $d\xi$-measure of a fundamental parallelotope. Hence an integral ideal $\mathfrak{a}$, a sublattice of index $N(\mathfrak{a})$, has covolume $N(\mathfrak{a})$. The measure $d\xi$ is the measure in all geometric volumes ($\mathrm{vol} = \mathrm{vol}_{d\xi}$) and in all integrals over the domain $\mathfrak{B}(P)$ introduced below, in particular in the function $V(\boldsymbol{\beta})$ of Section 4.3. The two are proportional, $\mathrm{vol}_{dx} = |D|\,\mathrm{vol}_{d\xi}$, since the coordinate change $x_j = \mathrm{Tr}(\alpha\omega_j) = \sum_l u_l\,\mathrm{Tr}(\omega_l\omega_j)$ is linear with matrix $\big(\mathrm{Tr}(\omega_l\omega_j)\big)_{l,j}$, whose determinant is D. The constant $|D|$, like the Jacobian of the coordinates $(\xi^{(1)}, \ldots, \xi^{(r_1+r_2)}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, enters only the constants implied by $\ll$ and $\asymp$.

Definition 4.1. For $\gamma \in K^\times$, there exist unique coprime integral ideals $\mathfrak{a}, \mathfrak{b}$ with $\gamma\mathfrak{D} = \mathfrak{b}\mathfrak{a}^{-1}$. We say that γ is *associated with* the ideal $\mathfrak{a}$, call $\mathfrak{a}$ the *denominator* of γ, and write $\gamma \to \mathfrak{a}$ (and $0 \to \mathcal{O}_K$). For a tuple $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_n) \in K^n$ with $\gamma_s \to \mathfrak{a}_s$, we say that $\boldsymbol{\gamma}$ is *associated with* the *common denominator*

$$\mathfrak{a}_{\boldsymbol{\gamma}} = \operatorname{lcm}(\mathfrak{a}_1, \dots, \mathfrak{a}_n),$$

the least common multiple of ideals.

Equivalently, an integral ideal $\mathfrak{a}$ satisfies $\gamma_s\mathfrak{a} \subseteq \mathfrak{D}^{-1}$ for all s if and only if $\mathfrak{a}_{\boldsymbol{\gamma}} \mid \mathfrak{a}$.

4.2.2 The Counting Function and Its Integral Representation

Definition 4.2. For $P \geq 1$, set

$$\mathcal{P}(P) = \left\{ x \in \mathcal{O}_K \;\middle|\; x^{(i)} > 0 \ (1 \leq i \leq r_1),\ |x^{(i)}| \leq P \ (1 \leq i \leq m) \right\},$$

and let

$$\mathfrak{B}(P) = \left\{ \xi \in K_{\mathbb{R}} \;\middle|\; \xi^{(i)} > 0 \ (1 \leq i \leq r_1),\ |\xi^{(i)}| \leq P \ (1 \leq i \leq m) \right\}$$

be the corresponding region of $K_{\mathbb{R}}$, so that $\mathcal{P}(P) = \mathcal{O}_K \cap \mathfrak{B}(P)$. The counting function of the Hilbert-Kamke system is

$$r(\boldsymbol{N}, P) = \# \left\{ (x_1, \dots, x_k) \in \mathcal{P}(P)^k \;\middle|\; \sum_{i=1}^{k} x_i^s = N_s,\ 1 \leq s \leq n \right\}.$$

The set $\mathcal{P}(P)$ is finite, because $\mathcal{O}_K$ is a lattice in $K_{\mathbb{R}}$ and $\mathfrak{B}(P)$ is bounded, and $\#\mathcal{P}(P) \asymp P^m$ by Lemma 4.6(iii) below. If $r(\boldsymbol{N}, P) > 0$, then N_s is totally positive and $\|N_s\| \leq kP^s$ for $1 \leq s \leq n$, so $\vartheta_s = N_s P^{-s}$ lies in a fixed bounded region of $K_{\mathbb{R}}$, as in [25, Theorem 7.2, p. 88].

Lemma 4.3 (cf. [25, Lemma 5.2, p. 59])**.** *For $\nu \in \mathcal{O}_K$, regarded in $K_{\mathbb{R}}$,*

$$\int_{U_m} E(\nu\alpha)\, dx = \begin{cases} 1, & \nu = 0, \\ 0, & \nu \neq 0. \end{cases}$$

Proof. Write $\nu = \sum_j a_j\omega_j$ with $a_j \in \mathbb{Z}$ and $\alpha = \sum_j x_j\rho_j$. By duality, $\operatorname{Tr}(\nu\alpha) = \sum_j a_j x_j$, so the integral factors as $\prod_j \int_0^1 e(a_j x_j)\, dx_j$, which is 1 if all $a_j = 0$ and 0 otherwise. □

Definition 4.4. For $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in K_{\mathbb{R}}^n$ and $P \geq 1$, set

$$S(\boldsymbol{\alpha}, P) = \sum_{x \in \mathcal{P}(P)} E\left(\sum_{s=1}^{n} \alpha_s x^s\right).$$

Expanding $S(\boldsymbol{\alpha}, P)^k$ and applying Lemma 4.3 in each of the n coordinates gives

$$r(\boldsymbol{N}, P) = \int_{U_m^n} S(\boldsymbol{\alpha}, P)^k E\left(-\sum_{s=1}^{n} N_s \alpha_s\right) d\boldsymbol{x}. \tag{4.1}$$

The integrand of (4.1) is periodic modulo $\mathfrak{D}^{-1}$ in each coordinate. Fix s and let $\psi \in \mathfrak{D}^{-1}$. Then for $x \in \mathcal{O}_K$ one has $\psi x^s \in \mathfrak{D}^{-1}$ and $N_s\psi \in \mathfrak{D}^{-1}$, so $E(\psi x^s) = E(N_s\psi) = 1$, so

$$\begin{aligned} S(\alpha_1, \ldots, \alpha_s + \psi, \ldots, \alpha_n, P) &= S(\boldsymbol{\alpha}, P), \\ E\Big(-\sum_{s'} N_{s'}\alpha_{s'} - N_s\psi\Big) &= E\Big(-\sum_{s'} N_{s'}\alpha_{s'}\Big). \end{aligned} \tag{4.2}$$

We may therefore regard the integrand as a function on the torus $\mathbb{T} = (K_{\mathbb{R}}/\mathfrak{D}^{-1})^n$, and U_m^n as a fundamental domain for $\mathbb{T}$. The measure $d\boldsymbol{x}$ on $K_{\mathbb{R}}^n$ descends to the Haar measure of total mass 1 on $\mathbb{T}$, and every integral over $\mathbb{T}$ or over a subset of $\mathbb{T}$ below is taken with respect to it.

4.2.3 Lemmas

From [15, Chapter 3], we use the unique factorization of fractional ideals, the multiplicativity $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ of the ideal norm, and $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$. The norm is extended to fractional ideals by $N(\mathfrak{gh}^{-1}) = N(\mathfrak{g})/N(\mathfrak{h})$, and it is still multiplicative. For a prime ideal $\wp$ and $x \in K^\times$, $v_\wp(x)$ denotes the exponent of $\wp$ in the factorization of (x). If $v_\wp(x) < v_\wp(y)$, then $v_\wp(x+y) = v_\wp(x)$, as one sees by comparing factorizations. We write $\wp^l \parallel \mathfrak{a}$ when $\wp^l \mid \mathfrak{a}$ and $\wp^{l+1} \nmid \mathfrak{a}$.

Lemma 4.5 (cf. [13, Chapters III, V]; [15, Chapter 3]; [25, Lemmas 2.1, 2.5, pp. 15–16])**.** *Let $\mathfrak{l}$ be a fractional ideal, $\mathfrak{c}$ and $\mathfrak{q}$ non-zero integral ideals, and $\varepsilon > 0$.*

(i) $\{\rho_1, \ldots, \rho_m\}$ is a $\mathbb{Z}$-basis of $\mathfrak{D}^{-1}$. Hence U_m contains exactly one representative of each class of $K_{\mathbb{R}}$ modulo $\mathfrak{D}^{-1}$, and $E(\psi\nu) = 1$ for all $\psi \in \mathfrak{D}^{-1}$ and $\nu \in \mathcal{O}_K$.

(ii) $[\mathfrak{l} : \mathfrak{lc}] = N(\mathfrak{c})$. *In particular, the group* $\mathcal{G}_\mathfrak{q} = \mathfrak{q}^{-1}\mathfrak{D}^{-1}/\mathfrak{D}^{-1}$ *has order* $N(\mathfrak{q})$.

(iii) Every $\mu \in \mathfrak{l}$, $\mu \neq 0$, *has* $|N_{K/\mathbb{Q}}(\mu)| \geq N(\mathfrak{l})$. *In particular, a non-zero* $\psi \in \mathfrak{D}^{-1}$ *has* $\|\psi\| \geq |D|^{-1/m}$.

(iv) For $\nu \in \mathcal{O}_K$, *the value* $E(\nu\gamma)$ *depends only on the class of* γ *in* $\mathcal{G}_\mathfrak{q}$, *and*

$$\sum_{\gamma \in \mathcal{G}_\mathfrak{q}} E(\nu\gamma) = \begin{cases} N(\mathfrak{q}), & \nu \in \mathfrak{q}, \\ 0, & \nu \notin \mathfrak{q}. \end{cases}$$

(v) There is $C_5 = C_5(K)$ *such that every non-zero integral ideal* $\mathfrak{a}$ *contains* $\mu \neq 0$ *with* $\|\mu\| \leq C_5 N(\mathfrak{a})^{1/m}$.

(vi) Multiplication by $\mu \in \mathcal{O}_K \setminus \{0\}$ *scales the measure* $d\xi$ *by* $|N_{K/\mathbb{Q}}(\mu)|$. *Hence the lattice* $\mu\mathcal{O}_K$ *has covolume* $|N_{K/\mathbb{Q}}(\mu)|$, *and* $[\mathfrak{a} : \mu\mathcal{O}_K] = |N_{K/\mathbb{Q}}(\mu)|/N(\mathfrak{a})$ *for* $\mu \in \mathfrak{a}$.

(vii) $d(\mathfrak{a}) \ll_\varepsilon N(\mathfrak{a})^\varepsilon$, *where* $d(\mathfrak{a})$ *is the number of integral ideals dividing* $\mathfrak{a}$.

Sketch of proof. (i) follows from the definition of the inverse different in Section 4.1 (see also [13, Chapter III]). Explicitly, $x = \sum_i c_i\rho_i$ has $c_i = \mathrm{Tr}(x\omega_i)$, and for $x \in K$, $\mathrm{Tr}(x\mathcal{O}_K) \subseteq \mathbb{Z}$ holds if and only if all $\mathrm{Tr}(x\omega_i) = c_i$ lie in $\mathbb{Z}$. The remaining claims follow by reducing the coordinates modulo 1, and from $\psi\nu \in \mathfrak{D}^{-1}$ together with the defining property $\mathrm{Tr}_{K/\mathbb{Q}}(\mathfrak{D}^{-1}) \subseteq \mathbb{Z}$ of the inverse different.

(ii) Multiplying by a non-zero $\psi \in \mathfrak{h}$ (for $\mathfrak{l} = \mathfrak{g}\mathfrak{h}^{-1}$) reduces to integral $\mathfrak{l}$, where $[\mathfrak{l} : \mathfrak{lc}] = [\mathcal{O}_K : \mathfrak{lc}]/[\mathcal{O}_K : \mathfrak{l}] = N(\mathfrak{lc})/N(\mathfrak{l}) = N(\mathfrak{c})$ by the multiplicativity of the ideal norm [15, Chapter 3].

(iii) $(\mu)\mathfrak{l}^{-1}$ is an integral ideal, so, by $N((\mu)) = |N_{K/\mathbb{Q}}(\mu)|$ (Section 4.1), $|N_{K/\mathbb{Q}}(\mu)| = N(\mathfrak{l})\,N\big((\mu)\mathfrak{l}^{-1}\big) \geq N(\mathfrak{l})$, and $N(\mathfrak{D}^{-1}) = 1/|D|$ (the norm of the different is the absolute discriminant, [13, Chapter III]) gives $\|\psi\|^m \geq |N_{K/\mathbb{Q}}(\psi)| \geq 1/|D|$.

(iv) is [25, Lemma 2.5, p. 16]. Alternatively, $\gamma \mapsto E(\nu\gamma)$ is a character of $\mathcal{G}_\mathfrak{q}$, and it is trivial if and only if $\mathrm{Tr}(\nu\mathfrak{q}^{-1}\mathfrak{D}^{-1}) \subseteq \mathbb{Z}$. Since the set $\nu\mathfrak{q}^{-1}\mathfrak{D}^{-1}$ is an $\mathcal{O}_K$-module, each of its elements x then satisfies $\mathrm{Tr}(x\mathcal{O}_K) \subseteq \mathbb{Z}$, that is, $x \in \mathfrak{D}^{-1}$ by the definition of the inverse different. Hence the condition becomes $\nu\mathfrak{q}^{-1}\mathfrak{D}^{-1} \subseteq \mathfrak{D}^{-1}$, that is, $(\nu)\mathfrak{q}^{-1} \subseteq \mathcal{O}_K$, which means $\nu \in \mathfrak{q}$. A non-trivial character sums to zero.

(v) Minkowski's theorem ([13, Chapter V]) applied to the set $\{\|\xi\| \leq R\}$, which is convex and symmetric about 0, and the lattice $\mathfrak{a}$ of covolume $N(\mathfrak{a})$. The set has $d\xi$-volume

$c_K R^m$, being a product of intervals and discs in the real coordinates of $K_{\mathbb{R}}$, up to the fixed Jacobian of the coordinate change, and $C_5^m = 2^{m+1}/c_K$.

(vi) In the real coordinates, multiplication by μ is block diagonal, with a block $(\mu^{(i)})$ at each real place and a 2×2 block of determinant $|\mu^{(i)}|^2$ at each complex pair, of total determinant $|N_{K/\mathbb{Q}}(\mu)|$ in absolute value. The index formula follows by comparing the covolumes of $\mu\mathcal{O}_K$, $\mathfrak{a}$ and $\mathcal{O}_K$.

(vii) is [25, Lemma 2.1, p. 15], via $d(\mathfrak{a}) \le d(N(\mathfrak{a}))^m$ and the rational divisor bound ([8, Theorem 315]). □

Lemma 4.6 (cf. [25, Lemma 2.1, p. 15] and [8, Theorem 315])**.** *Fix $\varepsilon > 0$ and let $P \ge 1$.*

(i) The number of integral ideals of norm q is $\ll_\varepsilon q^\varepsilon$.

(ii) For fixed $C \ge 1$, $C^{\#\{\wp \mid \mathfrak{a}\}} \ll_{\varepsilon,C,K} N(\mathfrak{a})^\varepsilon$, where $\#\{\wp \mid \mathfrak{a}\}$ is the number of distinct prime ideal divisors of $\mathfrak{a}$.

(iii) $\mathrm{vol}_{d\xi}\, \mathfrak{B}(P) \asymp P^m$, and $\#\mathcal{P}(P) \asymp P^m$ for $P \ge 2$. Consequently, $|S(\boldsymbol{\alpha}, P)| \ll P^m$.

(iv) For $R_1, \dots, R_n > 0$, the box $\{\boldsymbol{\beta} \in K_{\mathbb{R}}^n : \|\beta_s\| \le R_s\}$ has volume $\asymp \prod_{s=1}^n R_s^m$ in the n-fold product of $d\xi$.

(v) For $0 < R \le P$, let $\mathfrak{B}_R^+ = \{|\xi^{(i)}| \le P + R\ \forall i,\ \xi^{(i)} \ge -R\ (i \le r_1)\}$ and $\mathfrak{B}_R^- = \{\xi \in \mathfrak{B}(P-R) : \xi^{(i)} \ge R\ (i \le r_1)\}$. Then $\mathrm{vol}_{d\xi}\left(\mathfrak{B}_R^+ \setminus \mathfrak{B}_R^-\right) \ll RP^{m-1}$. Every point within $\|\cdot\|$-distance R of the boundary $\partial\mathfrak{B}(P)$ of $\mathfrak{B}(P)$ in $K_{\mathbb{R}}$ lies in $\mathfrak{B}_R^+$, and every point of $\mathfrak{B}_R^-$ has $\|\cdot\|$-distance $\ge R$ from the complement of $\mathfrak{B}(P)$.

Sketch of proof. (i) The counting function $a_K(q) = \#\{\mathfrak{a} : N(\mathfrak{a}) = q\}$ satisfies $a_K(q) \le d(q)^m$. An ideal of norm $q = \prod_p p^{a_p}$ factors over the at most m primes above each p, with exponents $e_{p,i}$ satisfying $\sum_i e_{p,i} f_{p,i} = a_p$, and the number of admissible exponent vectors is at most $(a_p+1)^m = d(p^{a_p})^m$. The claim follows from the rational divisor bound, as in Lemma 4.5(vii).

(ii) Let $X_0 = C^{2/\varepsilon}$. There are at most $M_0 = M_0(X_0, K)$ prime ideals of norm $\le X_0$, and each remaining prime divisor has $C < N(\wp)^{\varepsilon/2}$, so $C^{\#\{\wp \mid \mathfrak{a}\}} \le C^{M_0} \prod_{\wp^l \| \mathfrak{a}} N(\wp^l)^{\varepsilon/2} = C^{M_0} N(\mathfrak{a})^{\varepsilon/2}$.

(iii) In the real coordinates, $\mathfrak{B}(P)$ is the product of r_1 intervals $(0, P]$ and r_2 discs of radius P, of volume $\asymp P^m$ up to the fixed Jacobian. The translates $x + U_\omega$, $x \in \mathcal{P}(P)$, where $U_\omega = \{\sum_j u_j \omega_j : u_j \in [0,1)\}$ has $d\xi$-volume 1 and bounded diameter, are pairwise disjoint and contained in a region of volume $\ll P^m$, and $|S| \le \#\mathcal{P}(P)$. For the lower

bound, let $C_6 = m \max_j \|\omega_j\|$, and let a be the least integer greater than $P/4$, so that $P/4 < a \le P/4 + 1$. For integers $c_1, \dots, c_m$ with $|c_j| \le P/(4C_6)$, the number $y = \sum_j c_j \omega_j$ satisfies $\|y\| \le P/4$, and $x = a + y$ lies in $\mathcal{O}_K$ with $x^{(i)} \ge a - P/4 > 0$ for $i \le r_1$ and $|x^{(i)}| \le a + P/4 \le P/2 + 1 \le P$ for all i, because $P \ge 2$. Hence $x \in \mathcal{P}(P)$. Distinct tuples $(c_1, \dots, c_m)$ give distinct x, since $\omega_1, \dots, \omega_m$ is a basis. If $P \ge 4C_6$, there are at least $(2\lfloor P/(4C_6) \rfloor + 1)^m \ge (P/(4C_6))^m$ tuples, and if $2 \le P < 4C_6$, the bound $\#\mathcal{P}(P) \gg P^m$ is trivial because $1 \in \mathcal{P}(P)$. This proves $\#\mathcal{P}(P) \gg P^m$.

(iv) The box is a product over s of sets of volume $\asymp R_s^m$, as in (iii).

(v) Both $\mathfrak{B}_R^{\pm}$ are products of intervals and discs whose defining radii differ from those of $\mathfrak{B}(P)$ by at most $2R$. Writing the volume difference as a telescoping sum over the $r_1 + r_2$ factors gives $\ll RP^{m-1}$. The two inclusions follow coordinate by coordinate. □

4.2.4 Farey Dissection

Let $P \ge 2$, let κ be a number with $0 < \kappa \le 1$, to be chosen in Theorem 4.21, and let

$$\theta = \frac{1}{2\big(m(n+2)+1\big)}, \qquad t = P^{\theta}, \qquad T' = t^{\kappa} = P^{\theta\kappa}, \qquad c_0 = \tfrac{1}{2}|D|^{-1/m}. \tag{4.3}$$

The results before Theorem 4.21 hold for every such κ. Since $0 < \kappa \le 1$, we have $1 \le T' \le t$, and $T' \to \infty$ as $P \to \infty$. Define

$$\mathbf{\Gamma}(t) = \{\boldsymbol{\gamma} \in K^n \cap U_m^n \mid N(\mathfrak{a}_{\boldsymbol{\gamma}}) \le t^m\},$$

which is a finite set, because there are finitely many integral ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \le t^m$, and for each of them the coordinates γ_s lie in $U_m \cap \mathfrak{a}^{-1}\mathfrak{D}^{-1}$, a set of $N(\mathfrak{a})$ points by Lemma 4.5(i),(ii), and the box

$$\Omega = \big\{\boldsymbol{\beta} \in K_{\mathbb{R}}^n \;\big|\; \|\beta_s\| \le c_0 T' P^{-s},\ 1 \le s \le n\big\}, \tag{4.4}$$

which depends on P but not on $\boldsymbol{\gamma}$.

Definition 4.7. For $\boldsymbol{\gamma} \in \mathbf{\Gamma}(t)$, let $\mathbf{B}_{\boldsymbol{\gamma}} \subseteq \mathbb{T}$ be the image of $\boldsymbol{\gamma} + \Omega$ under the quotient map $K_{\mathbb{R}}^n \to \mathbb{T}$, that is, the set of the classes of the points $\boldsymbol{\gamma} + \boldsymbol{\beta}$ with $\boldsymbol{\beta} \in \Omega$.

The quotient map is injective on $\boldsymbol{\gamma} + \Omega$. If two points of $\boldsymbol{\gamma} + \Omega$ were congruent modulo $(\mathfrak{D}^{-1})^n$, their difference would have a coordinate $\psi \in \mathfrak{D}^{-1}$, $\psi \ne 0$, with $\|\psi\| \le 2c_0 T' P^{-s} = |D|^{-1/m} T' P^{-s}$. Since $T' \le t = P^{\theta}$ and $\theta < 1 \le s$, we have $T' P^{-s} < 1$, so $\|\psi\| < |D|^{-1/m}$,

contradicting Lemma 4.5(iii). The basic domains are defined on the torus, not in U_m^n, so that a box centred near the boundary of the fundamental domain is not cut, and the change of variables $\boldsymbol{\alpha} = \boldsymbol{\gamma} + \boldsymbol{\beta}$, $\boldsymbol{\beta} \in \Omega$, is valid on every arc.

The dissection differs from that of [25, Section 5.1] in one respect. The box Ω depends on P, through T', but not on the denominator $\mathfrak{a}_{\boldsymbol{\gamma}}$. So the major-arc integral of Section 4.3 factors exactly into a sum over $\boldsymbol{\Gamma}(t)$ and a single integral over Ω.

Lemma 4.8 (cf. [25, Lemma 5.1, p. 58])**.** *Let $P \geq 2$. If $\boldsymbol{\gamma}, \boldsymbol{\lambda} \in \boldsymbol{\Gamma}(t)$ are distinct, then $\mathbf{B}_{\boldsymbol{\gamma}} \cap \mathbf{B}_{\boldsymbol{\lambda}} = \emptyset$.*

Sketch of proof. Let $\mathfrak{a}, \mathfrak{b}$ be the common denominators associated with $\boldsymbol{\gamma}, \boldsymbol{\lambda}$ and fix s with $\gamma_s \neq \lambda_s$. A common point of the two domains, lifted to a point $\boldsymbol{\alpha} \in K_{\mathbb{R}}^n$, gives $\psi_s, \psi_s' \in \mathfrak{D}^{-1}$ with

$$\|\alpha_s - \gamma_s - \psi_s\| \leq c_0 T' P^{-s}, \qquad \|\alpha_s - \lambda_s - \psi_s'\| \leq c_0 T' P^{-s}.$$

Let $\mu = \gamma_s + \psi_s - \lambda_s - \psi_s'$. Since $\gamma_s \to \mathfrak{a}_s$ with $\mathfrak{a}_s \mid \mathfrak{a}$, we have $\gamma_s \in \mathfrak{a}^{-1}\mathfrak{D}^{-1}$, and $\psi_s \in \mathfrak{D}^{-1} \subseteq \mathfrak{a}^{-1}\mathfrak{D}^{-1}$, and similarly for λ_s, ψ_s' with $\mathfrak{b}$. Hence $\mu \in (\mathfrak{a}\mathfrak{b})^{-1}\mathfrak{D}^{-1}$. Moreover, $\mu \neq 0$, since otherwise $\gamma_s - \lambda_s = \psi_s' - \psi_s \in \mathfrak{D}^{-1}$, so $\gamma_s = \lambda_s$ by Lemma 4.5(i) ($\gamma_s, \lambda_s \in U_m$), a contradiction. Also, $\|\mu\| \leq 2c_0 T' P^{-s}$ by the triangle inequality. By Lemma 4.5(iii) and $N\big((\mathfrak{a}\mathfrak{b})^{-1}\mathfrak{D}^{-1}\big) = \big(|D|N(\mathfrak{a})N(\mathfrak{b})\big)^{-1}$,

$$\frac{1}{|D|N(\mathfrak{a})N(\mathfrak{b})} \leq \prod_{i=1}^{m} \big|\mu^{(i)}\big| \leq \big(2c_0 T' P^{-s}\big)^m = \frac{T'^m P^{-sm}}{|D|},$$

so $N(\mathfrak{a})N(\mathfrak{b}) \geq P^{sm} T'^{-m} \geq P^m t^{-m}$, since $T' \leq t$. But $N(\mathfrak{a})N(\mathfrak{b}) \leq t^{2m}$. This gives $P^m \leq t^{3m} = P^{3\theta m} < P^m$, since $3\theta m < 1$ by (4.3), a contradiction. □

Definition 4.9. The *major arcs* and *minor arcs* are

$$\mathbf{B} = \bigsqcup_{\boldsymbol{\gamma} \in \boldsymbol{\Gamma}(t)} \mathbf{B}_{\boldsymbol{\gamma}} \subseteq \mathbb{T}, \qquad \mathfrak{m} = \mathbb{T} \setminus \mathbf{B}.$$

By (4.2), the integral (4.1) may be computed on $\mathbb{T}$, and it splits as $\int_{\mathbf{B}} + \int_{\mathfrak{m}}$.

Remark 4.10. Wooley [30, Theorem 1.1] proves the asymptotic formula with the dominant main term $\sigma_{\mathbb{Z}}\, \tau_{\mathbb{Z}} P^{k - \frac{1}{2}n(n+1)}$ of Theorem 3.1 for the number of solutions of the Hilbert-Kamke system over $\mathbb{Q}$, for $n \geq 3$ and $k \geq n(n+1)$ and under the assumption of local solubility. Wooley [29, Section 15] outlines Vinogradov's mean value theorem for the ring of integers of an arbitrary number field, and an estimate of the minor arcs over K would

start from this mean value theorem. Since the estimate can be obtained from this work, we do not treat the minor arcs in this thesis. The lower bound for the singular series, that is, the local solubility of the system, depends only on the major arcs, and it is the subject of the rest of this thesis.

4.3 The Major-Arc Evaluation

This section reduces $\int_{\mathbf{B}}$ to a truncated singular series and a truncated singular integral (Lemma 4.16). Throughout,

$$Q = m\Big(k - \frac{n(n+1)}{2}\Big), \qquad \eta = \frac{k}{n} - n - 1.$$

4.3.1 Gauss Sums and the Singular Series

Definition 4.11. For $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_n) \in K^n$ let $\mathfrak{a} = \mathfrak{a}_{\boldsymbol{\gamma}}$ be the common denominator associated with $\boldsymbol{\gamma}$, and define

$$G(\boldsymbol{\gamma}) = \sum_{x \bmod \mathfrak{a}} E\left(\sum_{s=1}^{n} \gamma_s x^s\right).$$

On K, one has $E = e \circ \mathrm{Tr}_{K/\mathbb{Q}}$. The summand depends only on x modulo $\mathfrak{a}$. If $x \equiv y \pmod{\mathfrak{a}}$, then $x^s - y^s \in \mathfrak{a}$ and $\gamma_s(x^s - y^s) \in \gamma_s\mathfrak{a} \subseteq \mathfrak{D}^{-1}$, so $E(\gamma_s(x^s - y^s)) = 1$.

By Lemma 4.5(i), U_m^n contains exactly one representative of each class of K^n modulo $(\mathfrak{D}^{-1})^n$. The denominator of γ depends only on the class of γ modulo $\mathfrak{D}^{-1}$: if $\psi \in \mathfrak{D}^{-1}$, then $\psi\mathfrak{c} \subseteq \mathfrak{D}^{-1}$ for every integral ideal $\mathfrak{c}$, so γ and $\gamma + \psi$ have the same denominator. The number $N(\mathfrak{a}_{\boldsymbol{\gamma}})^{-k} G(\boldsymbol{\gamma})^k E(-\sum_s N_s\gamma_s)$ depends only on the class of $\boldsymbol{\gamma}$ modulo $(\mathfrak{D}^{-1})^n$. Indeed, if γ_s is replaced by $\gamma_s + \psi$ with $\psi \in \mathfrak{D}^{-1}$, then each term of $G(\boldsymbol{\gamma})$ is multiplied by $E(\psi x^s) = 1$ and the factor $E(-\sum_s N_s\gamma_s)$ is multiplied by $E(-N_s\psi) = 1$, by Lemma 4.5(i).

Definition 4.12 (Singular series)**.** For integral ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n$, write $\mathfrak{a}$ for their least common multiple and set

$$A(\mathfrak{a}_1, \dots, \mathfrak{a}_n) = N(\mathfrak{a})^{-k} \sideset{}{^*}\sum_{\gamma_1 \to \mathfrak{a}_1} \cdots \sideset{}{^*}\sum_{\gamma_n \to \mathfrak{a}_n} G(\boldsymbol{\gamma})^k E\left(-\sum_{s=1}^{n} N_s\gamma_s\right),$$

$\sum^*_{\gamma\to\mathfrak{c}}$ denoting summation over a set of representatives, modulo $\mathfrak{D}^{-1}$, of the elements of K with denominator exactly $\mathfrak{c}$ (well defined by the two invariance properties above). If the sum

$$\sum_{\mathfrak{a}_1,\dots,\mathfrak{a}_n} A(\mathfrak{a}_1,\dots,\mathfrak{a}_n),$$

extending over all n-tuples of integral ideals, converges absolutely, we define the *singular series* σ_K to be its value. Since K is fixed throughout, we write σ for σ_K. For $t \geq 1$ set

$$\sigma(t) = \sum_{\boldsymbol{\gamma}\in\boldsymbol{\Gamma}(t)} N(\mathfrak{a}_{\boldsymbol{\gamma}})^{-k} G(\boldsymbol{\gamma})^k E\Big(-\sum_{s=1}^{n} N_s\gamma_s\Big).$$

The absolute convergence of σ, for $k > n(n+1)$, is Theorem 4.20 of the next section.

The tuples $\boldsymbol{\gamma} \in \boldsymbol{\Gamma}(t)$ associated with the common denominator $\mathfrak{a}$ correspond bijectively to the tuples of classes with denominators of least common multiple $\mathfrak{a}$. Hence, by the definition of A,

$$\sigma(t) = \sum_{\substack{\mathfrak{a}_1,\dots,\mathfrak{a}_n \\ N(\mathrm{lcm}(\mathfrak{a}_1,\dots,\mathfrak{a}_n))\leq t^m}} A(\mathfrak{a}_1,\dots,\mathfrak{a}_n),$$

a partial sum of σ. We call $\sigma(t)$ the truncated singular series. Once the absolute convergence of σ is established, $\sigma(t) \to \sigma$ as $t \to \infty$.

4.3.2 An Approximation Lemma

Definition 4.13. For $\boldsymbol{\beta} \in K_{\mathbb{R}}^n$, set

$$V(\boldsymbol{\beta}) = \int_{\mathfrak{B}(P)} E\left(\sum_{s=1}^{n} \beta_s\xi^s\right) d\xi.$$

In particular, $|V(\boldsymbol{\beta})| \leq \int_{\mathfrak{B}(P)} d\xi \ll P^m$.

Lemma 4.14 (cf. [25, Lemma 5.6, p. 65])**.** *Let $\boldsymbol{\gamma} \in K^n$ be associated with the common denominator $\mathfrak{a}$, and regard $\boldsymbol{\gamma}$ as an element of $K_{\mathbb{R}}^n$ by embedding each coordinate. Then, for every $\boldsymbol{\beta} \in K_{\mathbb{R}}^n$,*

$$S(\boldsymbol{\gamma}+\boldsymbol{\beta}, P) = N(\mathfrak{a})^{-1} G(\boldsymbol{\gamma}) V(\boldsymbol{\beta}) + O\left(N(\mathfrak{a})^{1/m} P^{m-1}\Big(1 + \sum_{s=1}^{n} \|\beta_s\| P^s\Big)\right).$$

Proof. By Lemma 4.5(v), choose $\mu \in \mathfrak{a} \setminus \{0\}$ with $\|\mu\| \le C_5 N(\mathfrak{a})^{1/m}$. The sublattice $\mathfrak{n} = \mu\mathcal{O}_K \subseteq \mathfrak{a}$ has index $M = |N_{K/\mathbb{Q}}(\mu)|/N(\mathfrak{a}) \le C_5^m$ (Lemma 4.5(vi)), is spanned by $\mu\omega_1, \dots, \mu\omega_m$ with $\|\mu\omega_j\| \le \|\mu\|\|\omega_j\| \ll N(\mathfrak{a})^{1/m}$ (componentwise multiplication), and its fundamental parallelotope $\mathcal{F} = \{\sum_j u_j \mu\omega_j : u_j \in [0,1)\}$ is convex with

$$R := \operatorname{diam}_{\|\cdot\|} \mathcal{F} = \sup_{\xi,\zeta\in\mathcal{F}} \|\xi - \zeta\| \le \sum_j \|\mu\omega_j\| \ll N(\mathfrak{a})^{1/m},$$
$$\int_{\mathcal{F}} d\xi = |N_{K/\mathbb{Q}}(\mu)| \asymp N(\mathfrak{a}),$$

the volume again by Lemma 4.5(vi). If $R > P$, then $N(\mathfrak{a})^{1/m} P^{m-1} \gg RP^{m-1} > P^m$, and the assertion is trivial, because both $|S(\boldsymbol{\gamma}+\boldsymbol{\beta}, P)|$ and $N(\mathfrak{a})^{-1}|G(\boldsymbol{\gamma})V(\boldsymbol{\beta})|$ are $\ll P^m$ by Lemma 4.6(iii) and $|G(\boldsymbol{\gamma})| \le N(\mathfrak{a})$. So we may assume $R \le P$, as Lemma 4.6(v) requires.

Since the summand of S at $\boldsymbol{\gamma}$ is $\mathfrak{a}$-periodic in x (as $\gamma_s \mathfrak{a} \subseteq \mathfrak{D}^{-1}$),

$$S(\boldsymbol{\gamma}+\boldsymbol{\beta}, P) = \sum_{y \bmod \mathfrak{a}} E\Big(\sum_s \gamma_s y^s\Big) Z(y),$$
$$Z(y) = \sum_{\substack{x \equiv y \pmod{\mathfrak{a}} \\ x \in \mathcal{P}(P)}} E_{\boldsymbol{\beta}}(x), \qquad E_{\boldsymbol{\beta}}(\xi) = E\Big(\sum_s \beta_s \xi^s\Big).$$

Split the class $y + \mathfrak{a}$ into its M subclasses $y' + \mathfrak{n}$, and fix one subclass $y' + \mathfrak{n}$. The translates $x + \mathcal{F}$, $x \in y' + \mathfrak{n}$, which we call cells, tile $K_{\mathbb{R}}$. Call a cell *interior* if it is contained in $\mathfrak{B}(P)$, and *boundary* if it intersects $\partial\mathfrak{B}(P)$ and is not interior. For every $x \in (y' + \mathfrak{n}) \cap \mathcal{P}(P)$, the cell $x + \mathcal{F}$ is of one of the two kinds. By Lemma 4.6(v), every boundary cell lies in $\mathfrak{B}_R^+ \setminus \mathfrak{B}_R^-$, so the number of boundary cells is at most $\operatorname{vol}(\mathfrak{B}_R^+ \setminus \mathfrak{B}_R^-)/|N_{K/\mathbb{Q}}(\mu)| \ll RP^{m-1}/N(\mathfrak{a})$, and likewise the $d\xi$-volume of $\mathfrak{B}(P) \setminus \bigcup_{\text{interior}} (x + \mathcal{F})$ is $\ll RP^{m-1}$. Comparing sum and integral cell by cell, with $|E_{\boldsymbol{\beta}}| = 1$,

$$\Big| \sum_{\substack{x \in y' + \mathfrak{n} \\ x \in \mathcal{P}(P)}} E_{\boldsymbol{\beta}}(x) - \frac{1}{|N_{K/\mathbb{Q}}(\mu)|} \int_{\mathfrak{B}(P)} E_{\boldsymbol{\beta}}(\xi)\, d\xi \Big|$$
$$\ll \frac{RP^{m-1}}{N(\mathfrak{a})} + \sum_{\text{interior } x} \Big| E_{\boldsymbol{\beta}}(x) - \frac{1}{|N_{K/\mathbb{Q}}(\mu)|} \int_{x+\mathcal{F}} E_{\boldsymbol{\beta}}(\xi)\, d\xi \Big|.$$

For an interior cell, $|e(u) - e(v)| \le 2\pi|u - v|$ and the mean value theorem along the segment

(the cell is convex and contained in $\mathfrak{B}(P)$) give, for $\xi \in x + \mathcal{F}$,

$$|E_{\boldsymbol{\beta}}(x) - E_{\boldsymbol{\beta}}(\xi)| \;\ll\; R \sup \Big| \nabla \operatorname{Tr}\Big(\sum_s \beta_s \xi^s \Big) \Big| \;\ll\; R \sum_s s \|\beta_s\| P^{s-1}$$
$$\ll\; N(\mathfrak{a})^{1/m} \sum_s \|\beta_s\| P^{s-1},$$

the gradient taken in the real coordinates of $K_{\mathbb{R}}$ (differentiating the real-valued phase coordinatewise, using $|\xi^{(i)}| \le P$ on the cell, and the fixed coordinate change contributes a constant). The number of interior cells is at most $\operatorname{vol}\mathfrak{B}(P)/|N_{K/\mathbb{Q}}(\mu)| \ll P^m/N(\mathfrak{a})$ (Lemma 4.6(iii)). Summing over the $M \le C_5^m$ subclasses, using $M\,|N_{K/\mathbb{Q}}(\mu)|^{-1} = N(\mathfrak{a})^{-1}$ exactly,

$$Z(y) = \frac{1}{N(\mathfrak{a})} V(\boldsymbol{\beta}) + O\Big(P^{m-1} N(\mathfrak{a})^{1/m-1} \Big(1 + \sum_s \|\beta_s\| P^s \Big) \Big).$$

Summing over the $N(\mathfrak{a})$ classes y completes the proof. □

4.3.3 Reduction to the Truncated Singular Series and the Truncated Singular Integral

The substitution $\xi = P\xi'$ in V, for which $d\xi = P^m\, d\xi'$ and $\mathfrak{B}(P) = P\,\mathfrak{B}(1)$, gives

$$V(\boldsymbol{\beta}) = P^m V_1(\boldsymbol{\beta}'), \qquad \beta'_s = P^s \beta_s, \qquad V_1(\boldsymbol{\beta}') = \int_{\mathfrak{B}(1)} E\Big(\sum_{s=1}^{n} \beta'_s \xi^s \Big) d\xi,$$

and V_1 does not depend on P.

Definition 4.15. With $\vartheta_s = N_s P^{-s}$, the *normalized singular integral* of the Hilbert-Kamke system over K is

$$\tau_K = \int_{K_{\mathbb{R}}^n} V_1(\boldsymbol{\beta}')^k\, E\Big(-\sum_{s=1}^{n} \vartheta_s \beta'_s \Big) d\boldsymbol{x},$$

whenever the integral converges absolutely.

Lemma 4.16 (cf. [25, Lemmas 5.7 and 5.8, pp. 66–67])**.** *Let $k \ge 1$ and $P \ge 2$, with θ, t, T', Ω as in* (4.3), (4.4)*. Then*

$$\int_{\mathbf{B}} S(\boldsymbol{\alpha}, P)^k E\left(-\sum_{s=1}^{n} N_s \alpha_s \right) d\boldsymbol{x}$$
$$= \sigma(t)\, P^Q \int_{\substack{\boldsymbol{\beta}' \in K_{\mathbb{R}}^n \\ \|\beta'_s\| \le c_0 T' \;\; (1 \le s \le n)}} V_1(\boldsymbol{\beta}')^k\, E\Big(-\sum_{s=1}^{n} \vartheta_s \beta'_s \Big) d\boldsymbol{x} \;+\; O\big(P^{Q - 2\theta m} \big).$$

Proof. Throughout the proof, write

$$I_\Omega = \int_\Omega V(\boldsymbol{\beta})^k \, E\Big(- \sum_s N_s \beta_s \Big) d\boldsymbol{x}.$$

The substitution $\beta_s = P^{-s}\beta'_s$ is a diagonal linear map of determinant $P^{-\frac{1}{2}mn(n+1)}$, since multiplication by the scalar P^{-s} on $K_\mathbb{R}$ has determinant P^{-sm} in any linear coordinates, in particular for $d\boldsymbol{x}$. Together with $V(\boldsymbol{\beta}) = P^m V_1(\boldsymbol{\beta}')$, by the substitution $\xi = P\xi'$ inside V, and $N_s\beta_s = \vartheta_s\beta'_s$, it identifies I_Ω with P^Q times the inner integral of the statement, and Lemma 4.6(iii),(iv) give the trivial bound

$$|I_\Omega| \le \mathrm{vol}_{d\boldsymbol{x}}(\Omega)\, \sup|V|^k \ll \ \mathrm{vol}(\Omega)\, \sup|V|^k \ \ll \ T'^{mn} P^{-\frac{1}{2}mn(n+1)}\, P^{mk} = P^Q T'^{mn},$$

the first $\ll$ by the proportionality of dx and $d\xi$.

By Lemma 4.8, the injectivity of the quotient map on each box $\boldsymbol{\gamma}+\Omega$, and the periodicity (4.2) of the integrand,

$$\begin{aligned}\int_{\mathbf{B}} S(\boldsymbol{\alpha}, P)^k E\Big(- \sum_s N_s \alpha_s \Big) d\boldsymbol{x} \\ = \sum_{\boldsymbol{\gamma} \in \boldsymbol{\Gamma}(t)} E\Big(- \sum_s N_s \gamma_s \Big) \int_\Omega S(\boldsymbol{\gamma}+\boldsymbol{\beta}, P)^k \, E\Big(- \sum_s N_s \beta_s \Big) d\boldsymbol{x}.\end{aligned}$$

On Ω, we have $\sum_s \|\beta_s\| P^s \le nc_0 T' \ll T'$, so Lemma 4.14 gives, for $\boldsymbol{\gamma} \to \mathfrak{a}$,

$$S(\boldsymbol{\gamma}+\boldsymbol{\beta}, P) = N(\mathfrak{a})^{-1} G(\boldsymbol{\gamma}) V(\boldsymbol{\beta}) + O\big(N(\mathfrak{a})^{1/m} P^{m-1} T'\big),$$

and, since both $|S|$ and $|N(\mathfrak{a})^{-1}GV| \le |V|$ are $\ll P^m$ (Lemma 4.6(iii), and $|G| \le N(\mathfrak{a})$ trivially), the inequality $|z^k - w^k| \le k \max(|z|,|w|)^{k-1}|z-w|$ gives

$$S(\boldsymbol{\gamma}+\boldsymbol{\beta}, P)^k = N(\mathfrak{a})^{-k} G(\boldsymbol{\gamma})^k V(\boldsymbol{\beta})^k + O\big(P^{(k-1)m} N(\mathfrak{a})^{1/m} P^{m-1} T'\big).$$

Inserting this into the sum over $\boldsymbol{\Gamma}(t)$ and integrating over Ω, the main terms add up to $\sigma(t)\, I_\Omega$, by the definition of $\sigma(t)$. It remains to bound the total contribution of the error terms. There are at most $N(\mathfrak{a})^n$ tuples $\boldsymbol{\gamma} \in \boldsymbol{\Gamma}(t)$ associated with the common denominator $\mathfrak{a}$ (each γ_s lies in $U_m \cap \mathfrak{a}^{-1}\mathfrak{D}^{-1}$, a set of $N(\mathfrak{a})$ points by Lemma 4.5(i),(ii)), so, by Lemma 4.6(i),(iv) and $\sum_{q \le Y} q^c \le Y^{c+1}$ $(c \ge 0)$, the error terms contribute at most

$$\begin{aligned}\mathrm{vol}(\Omega)\, P^{km-1} T' \sum_{N(\mathfrak{a}) \le t^m} N(\mathfrak{a})^{n+\frac{1}{m}} \ \ll_\varepsilon \ P^{Q-1}\, T'^{mn+1}\, t^{\,m(n+1)+1+m\varepsilon} \\ \le \ P^{Q-1}\, t^{\,2mn+m+2+m\varepsilon} \ = \ P^{Q-\theta m(3-\varepsilon)},\end{aligned}$$

since $\mathrm{vol}(\Omega) \asymp T'^{mn} P^{-\frac{1}{2}mn(n+1)}$, $T' \le t$, and $\theta(2mn+m+2) = 1 - 3\theta m$ by (4.3). Taking $\varepsilon = 1$, the error terms contribute $O\big(P^{\,Q-2\theta m}\big)$. Hence

$$\int_{\mathbf{B}} S(\boldsymbol{\alpha}, P)^k E\Big(-\sum_s N_s \alpha_s\Big) d\boldsymbol{x} = \sigma(t)\, I_\Omega + O\big(P^{\,Q-2\theta m}\big),$$

and substituting $I_\Omega = P^{\,Q} \times$ (inner integral of the statement) completes the proof. $\square$

4.4 The Singular Series

The material before Theorem 4.20 follows [25].

4.4.1 Bounds for the Gauss Sums and Absolute Convergence

Let $\phi(\lambda) = \gamma_n \lambda^n + \cdots + \gamma_1 \lambda$ be a polynomial with coefficients $\gamma_s \in K$, not all zero, let $\mathfrak{c} = (\gamma_1, \ldots, \gamma_n)$ be the fractional ideal generated by the coefficients, and write $\mathfrak{c}\mathfrak{D} = \mathfrak{g}\mathfrak{q}^{-1}$ with integral ideals $\mathfrak{g}$, $\mathfrak{q}$ such that $(\mathfrak{g}, \mathfrak{q}) = \mathcal{O}_K$. The integral ideal $\mathfrak{q}$ is determined by the coefficients of ϕ, and we call it the ideal associated with ϕ. Comparing exponents prime by prime, for $\gamma_s \to \mathfrak{a}_s$, one has $v_\wp(\mathfrak{q}) = \max\big(0, -\min_s v_\wp(\gamma_s \mathfrak{D})\big) = \max_s v_\wp(\mathfrak{a}_s)$. That is, $\mathfrak{q}$ is the common denominator $\mathfrak{a}_{\boldsymbol{\gamma}}$ of Definition 4.1 associated with $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_n)$. The *complete exponential sum* of ϕ, as defined in [25, Section 2.1, p. 14], is

$$S(\phi, \mathfrak{q}) = \sum_{\lambda \bmod \mathfrak{q}} E\big(\phi(\lambda)\big),$$

and, by the above, for $\boldsymbol{\gamma} \neq \mathbf{0}$,

$$G(\boldsymbol{\gamma}) = S(\phi_{\boldsymbol{\gamma}}, \mathfrak{a}_{\boldsymbol{\gamma}}), \qquad \phi_{\boldsymbol{\gamma}}(\lambda) = \sum_{s=1}^{n} \gamma_s \lambda^s.$$

Lemma 4.17 ([25, Theorem 2.1 and Lemma 2.7, pp. 14 and 19], due to Hua [11])**.** *Let ϕ be as above with associated ideal $\mathfrak{q}$, and let $\varepsilon > 0$. Then*

$$|S(\phi, \mathfrak{q})| \;\ll_\varepsilon\; N(\mathfrak{q})^{1-\frac{1}{n}+\varepsilon},$$
$$\big|S(\phi, \wp^l)\big| \;\le\; n^{2m+1} N(\wp^l)^{1-\frac{1}{n}} \qquad \text{if } \mathfrak{q} = \wp^l,\ l \ge 1.$$

Lemma 4.18 ([25, Theorem 2.1, p. 14])**.** *Let $\wp$ be a prime ideal, $l \geq 1$, and let $\boldsymbol{\gamma}$ be associated with the common denominator $\wp^l$. Then*

$$|G(\boldsymbol{\gamma})| \leq n^{2m+1} N(\wp^l)^{1-\frac{1}{n}}.$$

Proof. Let $\mathcal{I} = \{s : \mathfrak{a}_s \neq \mathcal{O}_K\}$, where $\gamma_s \to \mathfrak{a}_s$. The set $\mathcal{I}$ is not empty, because $\operatorname{lcm}(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) = \wp^l \neq \mathcal{O}_K$. For $s \notin \mathcal{I}$, we have $\gamma_s \in \mathfrak{D}^{-1}$, so $E(\gamma_s x^s) = 1$ for every $x \in \mathcal{O}_K$, and these terms do not change the sum. Hence $G(\boldsymbol{\gamma}) = S(\phi_{\mathcal{I}}, \wp^l)$ for the polynomial $\phi_{\mathcal{I}}(\lambda) = \sum_{s \in \mathcal{I}} \gamma_s \lambda^s$, whose degree $n' = \max \mathcal{I}$ satisfies $1 \leq n' \leq n$ and whose coefficients γ_s, $s \in \mathcal{I}$, are non-zero. It suffices to verify that the hypothesis of Lemma 4.17 holds for $\phi_{\mathcal{I}}$, that is, that the coefficient ideal $\mathfrak{c} = (\gamma_s : s \in \mathcal{I})$ satisfies $\mathfrak{c}\mathfrak{D} = \mathfrak{g}(\wp^l)^{-1}$ with $(\mathfrak{g}, \wp) = \mathcal{O}_K$. For $s \in \mathcal{I}$, write $\gamma_s \mathfrak{D} = \mathfrak{b}_s \mathfrak{a}_s^{-1}$ with $(\mathfrak{a}_s, \mathfrak{b}_s) = \mathcal{O}_K$, so that $\mathfrak{a} := \operatorname{lcm}(\mathfrak{a}_s : s \in \mathcal{I}) = \wp^l$. Then

$$\mathfrak{c}\mathfrak{D} = \sum_{s \in \mathcal{I}} \gamma_s \mathfrak{D} = \Big(\sum_{s \in \mathcal{I}} \mathfrak{b}_s \, \mathfrak{a}\mathfrak{a}_s^{-1} \Big) \mathfrak{a}^{-1} =: \mathfrak{g}\, \mathfrak{a}^{-1},$$

and $\mathfrak{g}$ is an integral ideal. For the prime $\wp$, choose $s_0 \in \mathcal{I}$ with $\wp^l \parallel \mathfrak{a}_{s_0}$. Then $v_\wp(\mathfrak{b}_{s_0} \mathfrak{a}\mathfrak{a}_{s_0}^{-1}) = 0 + l - l = 0$, so $v_\wp(\mathfrak{g}) = \min_s v_\wp(\mathfrak{b}_s \mathfrak{a}\mathfrak{a}_s^{-1}) = 0$, that is, $(\mathfrak{g}, \wp) = \mathcal{O}_K$. The prime-power bound of Lemma 4.17, applied to $\phi_{\mathcal{I}}$ with modulus $\wp^l$, gives $|G(\boldsymbol{\gamma})| \leq {n'}^{2m+1} N(\wp^l)^{1-1/n'} \leq n^{2m+1} N(\wp^l)^{1-1/n}$, because $n' \leq n$ and $N(\wp^l) \geq 2$. □

Lemma 4.19 (cf. [25, Lemmas 6.2, 6.3, pp. 73–74])**.** *If* $\operatorname{lcm}(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$ *and* $\operatorname{lcm}(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ *are coprime, then*

$$A(\mathfrak{a}_1\mathfrak{b}_1, \ldots, \mathfrak{a}_n\mathfrak{b}_n) = A(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) A(\mathfrak{b}_1, \ldots, \mathfrak{b}_n).$$

Proof. Write $\mathfrak{A}, \mathfrak{B}$ for the two least common multiples. Then $(\mathfrak{a}_s, \mathfrak{b}_s) = \mathcal{O}_K$ for every s, and $\operatorname{lcm}(\mathfrak{a}_1\mathfrak{b}_1, \ldots, \mathfrak{a}_n\mathfrak{b}_n) = \mathfrak{A}\mathfrak{B}$ (compare $v_\wp$ prime by prime, where at every $\wp$ at most one of $v_\wp(\mathfrak{A}), v_\wp(\mathfrak{B})$ is positive).

Fix s and abbreviate $\mathfrak{a} = \mathfrak{a}_s$, $\mathfrak{b} = \mathfrak{b}_s$. The map

$$\mathfrak{a}^{-1}\mathfrak{D}^{-1}/\mathfrak{D}^{-1} \times \mathfrak{b}^{-1}\mathfrak{D}^{-1}/\mathfrak{D}^{-1} \longrightarrow (\mathfrak{a}\mathfrak{b})^{-1}\mathfrak{D}^{-1}/\mathfrak{D}^{-1}, \qquad (\alpha, \beta) \mapsto \alpha + \beta,$$

is well defined and injective. If $\alpha + \beta \in \mathfrak{D}^{-1}$, then $\alpha = (\alpha+\beta) - \beta \in \mathfrak{b}^{-1}\mathfrak{D}^{-1}$, so $\alpha\mathfrak{D}\mathfrak{a} \subseteq \mathcal{O}_K$ and $\alpha\mathfrak{D}\mathfrak{b} \subseteq \mathcal{O}_K$, so $\alpha\mathfrak{D}(\mathfrak{a} + \mathfrak{b}) = \alpha\mathfrak{D} \subseteq \mathcal{O}_K$, that is, $\alpha \in \mathfrak{D}^{-1}$, and then $\beta \in \mathfrak{D}^{-1}$. By Lemma 4.5(ii), both sides have $N(\mathfrak{a})N(\mathfrak{b})$ elements, so the map is a bijection. Moreover, the map multiplies the exact denominators. If $\alpha \to \mathfrak{d}_1$, $\beta \to \mathfrak{d}_2$ (so $\mathfrak{d}_1 \mid \mathfrak{a}$, $\mathfrak{d}_2 \mid \mathfrak{b}$, coprime), then, for $\wp \mid \mathfrak{d}_1$, we have $v_\wp(\alpha\mathfrak{D}) < 0 \leq v_\wp(\beta\mathfrak{D})$, so by the ultrametric property $v_\wp((\alpha + \beta)\mathfrak{D}) = v_\wp(\alpha\mathfrak{D})$. The same argument at $\wp \mid \mathfrak{d}_2$, and the trivial case at the other

prime ideals, give $\alpha+\beta\to\mathfrak{d}_1\mathfrak{d}_2$. Hence the map restricts to a bijection between pairs of classes with denominators exactly $(\mathfrak{a}_s,\mathfrak{b}_s)$ and classes with denominator exactly $\mathfrak{a}_s\mathfrak{b}_s$.

Since $(\mathfrak{A},\mathfrak{B})=\mathcal{O}_K$, there are $a\in\mathfrak{A}$, $b\in\mathfrak{B}$ with $a+b=1$. The map $x\mapsto(x \bmod \mathfrak{A}, x \bmod \mathfrak{B})$ is a ring isomorphism $\mathcal{O}_K/\mathfrak{A}\mathfrak{B}\to(\mathcal{O}_K/\mathfrak{A})\times(\mathcal{O}_K/\mathfrak{B})$. It is surjective because $x=yb+za$ satisfies $x\equiv y \pmod{\mathfrak{A}}$ and $x\equiv z \pmod{\mathfrak{B}}$, and its kernel is $\mathfrak{A}\cap\mathfrak{B}=\mathfrak{A}\mathfrak{B}$ (for x in the intersection, $x=xa+xb\in\mathfrak{A}\mathfrak{B}$).

Now let $\gamma_s=\alpha_s+\beta_s$ with α_s,β_s as above, and $x\equiv y \pmod{\mathfrak{A}}$, $x\equiv z \pmod{\mathfrak{B}}$. Then $x^s-y^s\in\mathfrak{A}$, and since $\alpha_s\mathfrak{A}=\alpha_s\mathfrak{a}_s\cdot\mathfrak{A}\mathfrak{a}_s^{-1}\subseteq\mathfrak{D}^{-1}$, we obtain $\alpha_s(x^s-y^s)\in\mathfrak{D}^{-1}$. Similarly, $\beta_s(x^s-z^s)\in\mathfrak{D}^{-1}$. By Lemma 4.5(i),

$$E\Big(\sum_s \gamma_s x^s\Big)=E\Big(\sum_s \alpha_s y^s\Big)E\Big(\sum_s \beta_s z^s\Big),$$

and summing over x by the isomorphism above gives $G(\boldsymbol{\gamma})=G(\boldsymbol{\alpha})G(\boldsymbol{\beta})$. Likewise, since $\gamma_s=\alpha_s+\beta_s$ exactly, $E(-\sum_s N_s\gamma_s)=E(-\sum_s N_s\alpha_s)\,E(-\sum_s N_s\beta_s)$.

Combining these facts with $N(\mathfrak{A}\mathfrak{B})^{-k}=N(\mathfrak{A})^{-k}N(\mathfrak{B})^{-k}$, we see that the sum defining $A(\mathfrak{a}_1\mathfrak{b}_1,\dots,\mathfrak{a}_n\mathfrak{b}_n)$ factors as claimed. □

For a single equation over $\mathcal{O}_K$, the corresponding results are Theorem 5.1 and Chapter 6 of Wang's book [25]; for the Hilbert-Kamke system over K, they are new.

Theorem 4.20. *Let $n\ge 2$, $k>n(n+1)$ and $\eta=\frac{k}{n}-n-1>0$. Then σ converges absolutely, and for every ε with $0<\varepsilon<\eta$ and every $Y\ge 1$,*

$$\sum_{\substack{\mathfrak{a}_1,\dots,\mathfrak{a}_n\\ N(\operatorname{lcm}(\mathfrak{a}_1,\dots,\mathfrak{a}_n))>Y}} \big|A(\mathfrak{a}_1,\dots,\mathfrak{a}_n)\big| \ll_\varepsilon Y^{-\eta+\varepsilon}.$$

Proof. The proof follows Wang's proof for a single equation [25, Section 6.2, pp. 73–74].

Fix a tuple $(\mathfrak{a}_1,\dots,\mathfrak{a}_n)$, let $\mathfrak{a}=\operatorname{lcm}(\mathfrak{a}_1,\dots,\mathfrak{a}_n)$, and let $\wp_1,\dots,\wp_r$ be the distinct prime divisors of $\mathfrak{a}$, so that

$$\mathfrak{a}=\prod_{j=1}^r \wp_j^{l_j},\quad l_j\ge 1,\qquad \mathfrak{a}_s=\prod_{j=1}^r \wp_j^{l_{s,j}},\quad 0\le l_{s,j}\le l_j,$$

where no other prime divides any $\mathfrak{a}_s$ (as $\mathfrak{a}_s\mid\mathfrak{a}$), and $l_j=\max_s l_{s,j}$ by the definition of the least common multiple. We first show that

$$A(\mathfrak{a}_1,\dots,\mathfrak{a}_n)=\prod_{j=1}^r A\big(\wp_j^{l_{1,j}},\dots,\wp_j^{l_{n,j}}\big), \tag{4.5}$$

by induction on r. For $r = 0$, both sides equal 1: the right-hand side is the empty product, and $A(\mathcal{O}_K, \dots, \mathcal{O}_K) = 1$ because the only class with denominator $\mathcal{O}_K$ is $\gamma = 0$, for which $G(\mathbf{0}) = 1$. For $r = 1$, there is nothing to prove. For $r \geq 2$, write $\mathfrak{a}_s = \mathfrak{b}_s\mathfrak{c}_s$ with $\mathfrak{b}_s = \prod_{j<r} \wp_j^{l_{s,j}}$ and $\mathfrak{c}_s = \wp_r^{l_{s,r}}$. Then $\operatorname{lcm}(\mathfrak{b}_1, \dots, \mathfrak{b}_n) = \prod_{j<r} \wp_j^{l_j}$ and $\operatorname{lcm}(\mathfrak{c}_1, \dots, \mathfrak{c}_n) = \wp_r^{l_r}$ are coprime, so Lemma 4.19 gives $A(\mathfrak{a}_1, \dots, \mathfrak{a}_n) = A(\mathfrak{b}_1, \dots, \mathfrak{b}_n)\, A(\mathfrak{c}_1, \dots, \mathfrak{c}_n)$, and (4.5) follows by applying the induction hypothesis to $(\mathfrak{b}_1, \dots, \mathfrak{b}_n)$.

We next estimate a single factor of (4.5). Fix j and abbreviate $\wp = \wp_j$, $l_s = l_{s,j}$ and $l = l_j = \max_s l_s \geq 1$. By the definition of A,

$$A(\wp^{l_1}, \dots, \wp^{l_n}) = N(\wp^l)^{-k} \sideset{}{^*}\sum_{\gamma_1 \to \wp^{l_1}} \cdots \sideset{}{^*}\sum_{\gamma_n \to \wp^{l_n}} G(\boldsymbol{\gamma})^k E\Big(-\sum_{s=1}^{n} N_s\gamma_s\Big).$$

By Lemma 4.5(ii), the classes γ_s with denominator exactly $\wp^{l_s}$ lie among the $N(\wp^{l_s})$ classes of $\wp^{-l_s}\mathfrak{D}^{-1}/\mathfrak{D}^{-1}$, so the sum contains at most $\prod_s N(\wp^{l_s}) \leq N(\wp^l)^n$ terms. Every tuple $\boldsymbol{\gamma}$ occurring in the sum has denominators exactly $\wp^{l_s}$, hence common denominator exactly $\wp^{\max_s l_s} = \wp^l$, so that Lemma 4.18 gives $|G(\boldsymbol{\gamma})|^k \leq \big(n^{2m+1} N(\wp^l)^{1-\frac{1}{n}}\big)^k$. Since $|E(-\sum_s N_s\gamma_s)| = 1$, it follows that

$$\big|A(\wp^{l_1}, \dots, \wp^{l_n})\big| \leq N(\wp^l)^{-k} \cdot N(\wp^l)^n \cdot \big(n^{2m+1} N(\wp^l)^{1-\frac{1}{n}}\big)^k = n^{(2m+1)k}\, N(\wp^l)^{\,n-\frac{k}{n}}. \tag{4.6}$$

Note that

$$n - \frac{k}{n} = -1 - \Big(\frac{k}{n} - n - 1\Big) = -1 - \eta \;<\; -1,$$

since $k > n(n+1)$.

Multiplying these bounds over $j = 1, \dots, r$ and using $\prod_j N(\wp_j^{l_j})^{\,n-k/n} = N(\mathfrak{a})^{\,n-k/n}$, we obtain

$$\big|A(\mathfrak{a}_1, \dots, \mathfrak{a}_n)\big| \leq \big(n^{(2m+1)k}\big)^r\, N(\mathfrak{a})^{\,n-\frac{k}{n}}.$$

Since the constant $n^{(2m+1)k}$ does not depend on $\wp_j$, Lemma 4.6(ii), applied with $C = n^{(2m+1)k}$, gives $C^r \ll_\varepsilon N(\mathfrak{a})^\varepsilon$, and therefore

$$\big|A(\mathfrak{a}_1, \dots, \mathfrak{a}_n)\big| \;\ll_\varepsilon\; N(\mathfrak{a})^{\,n-\frac{k}{n}+\varepsilon} = N(\mathfrak{a})^{-1-\eta+\varepsilon}, \tag{4.7}$$

uniformly over all tuples with least common multiple $\mathfrak{a}$.

Now let $0 < \varepsilon < \eta/3$. If $\operatorname{lcm}(\mathfrak{a}_1, \dots, \mathfrak{a}_n) = \mathfrak{a}$, then each $\mathfrak{a}_s$ divides $\mathfrak{a}$, so the number of tuples with a given least common multiple $\mathfrak{a}$ is at most $d(\mathfrak{a})^n \ll_\varepsilon N(\mathfrak{a})^\varepsilon$ (Lemma 4.5(vii)),

and the number of ideals $\mathfrak{a}$ with $N(\mathfrak{a}) = q$ is $\ll_\varepsilon q^\varepsilon$ (Lemma 4.6(i)). Grouping the tuples by $\mathfrak{a}$, then by $q = N(\mathfrak{a})$, and inserting (4.7),

$$\sum_{\substack{\mathfrak{a}_1,\dots,\mathfrak{a}_n \\ N(\mathrm{lcm})>Y}} |A| \;\le\; \sum_{q>Y} \sum_{\substack{\mathfrak{a} \\ N(\mathfrak{a})=q}} \sum_{\substack{\mathfrak{a}_1,\dots,\mathfrak{a}_n \\ \mathrm{lcm}=\mathfrak{a}}} |A| \ll_\varepsilon \sum_{q>Y} q^\varepsilon \cdot q^\varepsilon \cdot q^{-1-\eta+\varepsilon} = \sum_{q>Y} q^{-1-\eta+3\varepsilon}.$$

Since $\varepsilon < \eta/3$, the exponent $-1-\eta+3\varepsilon$ is strictly less than -1. Here the hypothesis $k > n(n+1)$, that is, $\eta > 0$, is used again. Comparison with the integral gives, for $Y \ge 1$,

$$\sum_{q>Y} q^{-1-\eta+3\varepsilon} \;\le\; Y^{-1-\eta+3\varepsilon} + \int_Y^\infty u^{-1-\eta+3\varepsilon}\,du \;\le\; \Big(1 + \frac{1}{\eta-3\varepsilon}\Big)\, Y^{-\eta+3\varepsilon}.$$

Taking $Y = 1$ and adding the term $A(\mathcal{O}_K,\dots,\mathcal{O}_K) = 1$ shows that the sum of $|A(\mathfrak{a}_1,\dots,\mathfrak{a}_n)|$ over all tuples is finite. Hence σ converges absolutely. Let ε with $0 < \varepsilon < \eta$ be given. The estimate above, applied with $\varepsilon/3$ in place of ε, gives $\sum_{N(\mathrm{lcm})>Y} |A| \ll_\varepsilon Y^{-\eta+\varepsilon}$. □

4.4.2 The Major-Arc Asymptotic

Theorem 4.21. *Let $n \ge 2$, $k > n(n+1)$ and $P \ge 2$. Recall $Q = m\big(k - \frac{n(n+1)}{2}\big)$ and $\eta = \frac{k}{n} - n - 1$. Let θ, t and $T' = t^\kappa$ be as in (4.3) with*

$$\kappa = \min\Big(1,\ \frac{\eta}{4n}\Big),$$

and let $\delta_0 = \theta m \min\big(2,\ \frac{\eta}{4}\big) > 0$. Then

$$\int_{\mathbf{B}} S(\boldsymbol{\alpha}, P)^k E\left(-\sum_{s=1}^n N_s \alpha_s\right) d\boldsymbol{x}$$
$$= \sigma\, P^Q \int_{\substack{\boldsymbol{\beta}' \in K_{\mathbb{R}}^n \\ \|\beta_s'\| \le c_0 T' \ (1\le s\le n)}} V_1(\boldsymbol{\beta}')^k\, E\Big(-\sum_{s=1}^n \vartheta_s \beta_s'\Big) d\boldsymbol{x} \;+\; O\big(P^{Q-\delta_0}\big),$$

the inner integral being the truncated singular integral, the truncation of τ_K to the box $\{\|\beta_s'\| \le c_0 T'\}$.

Proof. The proof follows Wang's proof for a single equation [25, Theorem 5.1, p. 60]. Write

$$J_0 = \int_{\substack{\boldsymbol{\beta}' \in K_{\mathbb{R}}^n \\ \|\beta_s'\| \le c_0 T' \ (1\le s\le n)}} V_1(\boldsymbol{\beta}')^k\, E\Big(-\sum_{s=1}^n \vartheta_s \beta_s'\Big) d\boldsymbol{x}$$

for the inner integral of the statement, so that Lemma 4.16 becomes

$$\int_{\mathbf{B}} S(\boldsymbol{\alpha},P)^k E\Big(-\sum_{s=1}^{n} N_s\alpha_s\Big)d\boldsymbol{x} = \sigma(t)\,P^Q J_0 + O\big(P^{Q-2\theta m}\big). \tag{4.8}$$

It remains to replace $\sigma(t)$ by σ in (4.8).

We first show that

$$|J_0| \;\ll\; T'^{mn} \;\le\; t^{m\eta/4}. \tag{4.9}$$

Indeed, for every $\boldsymbol{\beta}' \in K_{\mathbb{R}}^n$,

$$|V_1(\boldsymbol{\beta}')| \;\le\; \int_{\mathfrak{B}(1)} d\xi \;=\; \mathrm{vol}_{d\xi}\,\mathfrak{B}(1) \;\ll\; 1$$

by Lemma 4.6(iii) applied with $P=1$, so the integrand of J_0 is bounded, and the domain of integration is the box $\{\boldsymbol{\beta}' \in K_{\mathbb{R}}^n : \|\beta_s'\| \le c_0T',\ 1\le s\le n\}$, whose $d\boldsymbol{x}$-volume is $\ll T'^{mn}$ by Lemma 4.6(iv) (with $R_s = c_0T'$ for all s) and the proportionality $\mathrm{vol}_{dx} = |D|\,\mathrm{vol}_{d\xi}$ of Section 4.2. Hence $|J_0| \ll T'^{mn}$, and $T'^{mn} = t^{\kappa mn} \le t^{m\eta/4}$ because $\kappa \le \eta/(4n)$. The bound (4.9) follows.

We next estimate $\sigma(t)-\sigma$. By Theorem 4.20, σ converges absolutely. By the identity $\sigma(t) = \sum_{N(\mathrm{lcm})\le t^m} A$ of Section 4.3, the difference $\sigma - \sigma(t)$ is the sum of $A(\mathfrak{a}_1,\dots,\mathfrak{a}_n)$ over the tuples with $N(\mathrm{lcm}(\mathfrak{a}_1,\dots,\mathfrak{a}_n)) > t^m$, so

$$|\sigma(t)-\sigma| \;\le \sum_{\substack{\mathfrak{a}_1,\dots,\mathfrak{a}_n \\ N(\mathrm{lcm}(\mathfrak{a}_1,\dots,\mathfrak{a}_n))>t^m}} \big|A(\mathfrak{a}_1,\dots,\mathfrak{a}_n)\big|.$$

Applying the tail estimate of Theorem 4.20 with $Y = t^m$ and $\varepsilon = \eta/2$, which is admissible because the hypothesis $k > n(n+1)$ gives $\eta > 0$, we obtain

$$|\sigma(t)-\sigma| \;\ll\; (t^m)^{-\eta+\eta/2} = t^{-m\eta/2}. \tag{4.10}$$

Combining (4.9) and (4.10) with $t = P^\theta$ from (4.3),

$$\big|\sigma(t)\,P^Q J_0 - \sigma\,P^Q J_0\big| = |\sigma(t)-\sigma|\cdot P^Q\,|J_0| \;\ll\; P^Q\,t^{-m\eta/2}\,t^{m\eta/4} = P^{Q-\theta m\eta/4}.$$

Substituting this into (4.8),

$$\int_{\mathbf{B}} S(\boldsymbol{\alpha},P)^k E\Big(-\sum_{s=1}^{n} N_s\alpha_s\Big)d\boldsymbol{x} = \sigma\,P^Q J_0 + O\big(P^{Q-\theta m\eta/4}\big) + O\big(P^{Q-2\theta m}\big),$$

and both error terms are $O(P^{Q-\delta_0})$ for $\delta_0 = \theta m \min\big(2,\tfrac{\eta}{4}\big)$, which is positive since $\theta > 0$ and, by the hypothesis $k > n(n+1)$, $\eta > 0$. $\square$

The integral J_0 in Theorem 4.21 is the integral of Definition 4.15 taken over the box $\{\|\beta'_s\| \le c_0 T'\}$, which expands to $K_{\mathbb{R}}^n$ as $P \to \infty$, and J_0 tends to τ_K as $P \to \infty$, uniformly in $N_1, \dots, N_n$, as over $\mathbb{Q}$; we omit the proof. Following the same argument as in the case of $\mathbb{Q}$ (Lemma 3.10), under the growth condition, τ_K has a positive lower bound independent of P and $N_1, \dots, N_n$, so we do not treat it in this thesis.

4.4.3 Euler Product and Local Densities

Lemma 4.22 (cf. [25, Lemma 6.1, p. 73])**.** *Let $n \ge 2$ and $k > n(n+1)$. Then*

$$\sigma = \prod_{\wp} \sigma_\wp, \qquad \sigma_\wp = \sum_{e_1 \ge 0} \cdots \sum_{e_n \ge 0} A(\wp^{e_1}, \dots, \wp^{e_n}),$$

the product being over all prime ideals of $\mathcal{O}_K$ and absolutely convergent.

Proof. By Theorem 4.20, the family $\{A(\mathfrak{a}_1, \dots, \mathfrak{a}_n)\}$ is absolutely summable, and by (4.5) each term factors over prime powers. Since $\sigma_\wp - 1$ is the sum of $A(\wp^{e_1}, \dots, \wp^{e_n})$ over the tuples $(e_1, \dots, e_n) \ne (0, \dots, 0)$,

$$\sum_{\wp} |\sigma_\wp - 1| \ \le \sum_{\substack{\mathfrak{a}_1, \dots, \mathfrak{a}_n \\ \operatorname{lcm}(\mathfrak{a}_1, \dots, \mathfrak{a}_n) \ne \mathcal{O}_K}} \left| A(\mathfrak{a}_1, \dots, \mathfrak{a}_n) \right| < \infty,$$

so the product $\prod_\wp \sigma_\wp$ converges absolutely. Expanding the finite product $\prod_{N(\wp) \le y} \sigma_\wp$ and comparing with σ, the difference is bounded by the tail $\sum_{N(\operatorname{lcm}) > y} |A| \to 0$ as $y \to \infty$. □

Definition 4.23. For a non-zero integral ideal $\mathfrak{q}$ and $x_1, \dots, x_k$ running over a complete residue system modulo $\mathfrak{q}$, let $W(\mathfrak{q}, k)$ denote the number of solutions of

$$x_1^s + \cdots + x_k^s \equiv N_s \pmod{\mathfrak{q}}, \qquad 1 \le s \le n.$$

Theorem 4.24 (cf. [25, Lemma 6.5, p. 75])**.** *Let $n \ge 2$. For every non-zero integral ideal $\mathfrak{q}$,*

$$W(\mathfrak{q}, k) = N(\mathfrak{q})^{k-n} \sum_{\substack{\mathfrak{b}_1, \dots, \mathfrak{b}_n \\ \operatorname{lcm}(\mathfrak{b}_1, \dots, \mathfrak{b}_n) \mid \mathfrak{q}}} A(\mathfrak{b}_1, \dots, \mathfrak{b}_n).$$

Consequently, for $k > n(n+1)$ and every prime ideal $\wp$,

$$\sigma_\wp = \lim_{h \to \infty} N(\wp)^{h(n-k)} W(\wp^h, k).$$

Proof. For every s, apply Lemma 4.5(iv) with $\nu = x_1^s + \cdots + x_k^s - N_s$ and sum over $(x_1, \ldots, x_k) \in (\mathcal{O}_K/\mathfrak{q})^k$. The summand $E(\nu\gamma_s)$ depends only on the x_i modulo $\mathfrak{q}$, since ν then changes by elements of $\mathfrak{q}$ and $\gamma_s\mathfrak{q} \subseteq \mathfrak{D}^{-1}$. Expanding the n-fold product of the sums of Lemma 4.5(iv) and collecting, for every fixed $\boldsymbol{\gamma}$, the sum over $x_1, \ldots, x_k$,

$$W(\mathfrak{q}, k) = N(\mathfrak{q})^{-n} \sum_{\gamma_1 \in \mathcal{G}_\mathfrak{q}} \cdots \sum_{\gamma_n \in \mathcal{G}_\mathfrak{q}} T(\boldsymbol{\gamma})^k E\left(-\sum_s N_s\gamma_s\right),$$

$$T(\boldsymbol{\gamma}) = \sum_{x \bmod \mathfrak{q}} E\left(\sum_s \gamma_s x^s\right),$$

where $\mathcal{G}_\mathfrak{q} = \mathfrak{q}^{-1}\mathfrak{D}^{-1}/\mathfrak{D}^{-1}$ (Lemma 4.5(iv)).

Each class $\gamma_s \in \mathcal{G}_\mathfrak{q}$ has an exact denominator $\mathfrak{b}_s \mid \mathfrak{q}$, and conversely the classes with denominator exactly $\mathfrak{b}_s$ are those appearing in the definition of A. Fix a tuple $(\mathfrak{b}_1, \ldots, \mathfrak{b}_n)$ and let $\mathfrak{L} = \operatorname{lcm}(\mathfrak{b}_1, \ldots, \mathfrak{b}_n) \mid \mathfrak{q}$. The summand of T depends only on x modulo $\mathfrak{L}$ (as $\gamma_s(x^s - y^s) \in \gamma_s\mathfrak{b}_s \cdot \mathfrak{L}\mathfrak{b}_s^{-1} \subseteq \mathfrak{D}^{-1}$ for $x \equiv y \pmod{\mathfrak{L}}$), and the reduction $\mathcal{O}_K/\mathfrak{q} \to \mathcal{O}_K/\mathfrak{L}$ is surjective, and each of its fibres has $N(\mathfrak{q})/N(\mathfrak{L})$ elements (Lemma 4.5(ii)). Hence

$$T(\boldsymbol{\gamma}) = \frac{N(\mathfrak{q})}{N(\mathfrak{L})} G(\boldsymbol{\gamma}).$$

Substituting and comparing with the definition of A gives the first formula. For the second, take $\mathfrak{q} = \wp^h$. The formula becomes

$$N(\wp)^{h(n-k)} W(\wp^h, k) = \sum_{\substack{e_1, \ldots, e_n \geq 0 \\ \max_s e_s \leq h}} A(\wp^{e_1}, \ldots, \wp^{e_n}),$$

and the right side converges to $\sigma_\wp$ as $h \to \infty$ by Theorem 4.20. □

4.5 Local Solubility and the Lower Bound for the Singular Series

This section proves Theorem 4.30, the analogue of [25, Theorem 6.1, p. 72]. Recall that $k > n(n+1)$ and $\eta = \frac{k}{n} - n - 1$ throughout, and that, by Theorem 4.24, $\sigma_\wp = \lim_{h\to\infty} N(\wp)^{h(n-k)} W(\wp^h, k)$.

Lemma 4.25 (cf. [25, Lemma 6.4, p. 75])**.** *Let $n \geq 2$ and $k > n(n+1)$, and let $\wp$ be a prime ideal. If there are $c_\wp > 0$ and $h_\wp \geq 1$ such that, for all $h \geq h_\wp$,*

$$W(\wp^h, k) \;\geq\; c_\wp N(\wp)^{h(k-n)},$$

then $\sigma_\wp \geq c_\wp$.

Proof. Immediate from Theorem 4.24. □

We work in the completion. Let $\mathcal{O}_\wp$ denote the completion of the localization of $\mathcal{O}_K$ at $\wp$. This is a complete discrete valuation ring with maximal ideal generated by a uniformizer ϖ, residue field of $N(\wp)$ elements, and normalized valuation $v_\wp$, which extends the valuation $v_\wp$ of Section 4.2. The natural map induces a ring isomorphism $\mathcal{O}_K/\wp^u \cong \mathcal{O}_\wp/\varpi^u\mathcal{O}_\wp$ for every $u \geq 1$ (see [13, Chapter II]), so $W(\wp^u, k)$ counts solutions in $(\mathcal{O}_\wp/\varpi^u)^k$.

Definition 4.26. Let $\boldsymbol{x} = (x_1, \ldots, x_k)$ satisfy

$$x_1^s + \cdots + x_k^s \equiv N_s \pmod{\wp^u}, \qquad 1 \leq s \leq n.$$

For $1 \leq i_1 < \cdots < i_n \leq k$, let

$$J(\boldsymbol{x}, i_1, \ldots, i_n) = \det\big(s\, x_{i_j}^{s-1}\big)_{1 \leq s,j \leq n} = n! \prod_{1 \leq j < j' \leq n} \big(x_{i_{j'}} - x_{i_j}\big),$$

the second equality by extracting the factor s from the s-th row and evaluating the Vandermonde determinant $\det\big(x_{i_j}^{s-1}\big)_{1 \leq s,j \leq n}$. Let

$$\ell(\boldsymbol{x}) = \min_{1 \leq i_1 < \cdots < i_n \leq k} v_\wp\big(J(\boldsymbol{x}, i_1, \ldots, i_n)\big) \in \mathbb{Z}_{\geq 0} \cup \{\infty\},$$

the minimum over all choices of n indices. The solution $\boldsymbol{x}$ is *non-singular of level ℓ* if $\ell(\boldsymbol{x}) = \ell < \infty$ and $u \geq 2\ell + 1$.

The lifting is by the quantitative multivariate Hensel lemma (Greenberg [5, §3, Lemma 2, p. 63], who calls it Newton's lemma). If $\mathcal{O}$ is a complete discrete valuation ring with uniformizer ϖ and valuation v, if $F = (F_1, \ldots, F_n) \in \mathcal{O}[z_1, \ldots, z_n]^n$, and if $a \in \mathcal{O}^n$ satisfies $v(F_s(a)) \geq 2\ell + 1$ for all s, where $\ell = v\big(\det DF(a)\big) < \infty$ and $DF = (\partial F_s/\partial z_j)_{s,j}$, then there exists $\xi \in \mathcal{O}^n$ with $F(\xi) = 0$ and $\xi \equiv a \pmod{\varpi^{\ell+1}}$.

Lemma 4.27 (cf. [5, §3, Lemma 2] and [25, Lemma 6.7, p. 79])**.** *Let $k \geq n$ and $\ell \geq 0$. If the congruence system has a non-singular solution of level ℓ modulo $\wp^{2\ell+1}$, then, for all $h \geq 2\ell+1$,*

$$W(\wp^h, k) \;\geq\; N(\wp)^{(h-2\ell-1)(k-n)}.$$

Moreover, at least $N(\wp)^{(h-2\ell-1)(k-n)}$ of the solutions modulo $\wp^h$ are congruent to the given solution modulo $\wp^{\ell+1}$.

Proof. Let $\boldsymbol{x}^0 \in \mathcal{O}_\wp^k$ reduce to the given solution, and choose indices $i_1 < \cdots < i_n$ at which the minimum in the definition of $\ell(\boldsymbol{x})$ is attained, so that $v_\wp\big(J(\boldsymbol{x}^0, i_1, \ldots, i_n)\big) = \ell$ (the valuation of J depends only on $\boldsymbol{x}^0$ modulo $\varpi^{2\ell+1}$, since $2\ell+1 > \ell$). Write $\boldsymbol{x} = (\boldsymbol{z}, \boldsymbol{y})$ with $\boldsymbol{z} = (x_{i_1}, \ldots, x_{i_n})$ and $\boldsymbol{y}$ the remaining $k-n$ free coordinates, and let $F_s(\boldsymbol{z}, \boldsymbol{y}) = \sum_i x_i^s - N_s$.

Fix any $\boldsymbol{y} \in \mathcal{O}_\wp^{k-n}$ with $\boldsymbol{y} \equiv \boldsymbol{y}^0 \pmod{\varpi^{2\ell+1}}$. The map $g(\boldsymbol{z}) := F(\boldsymbol{z}, \boldsymbol{y})$ satisfies

$$v_\wp\big(g_s(\boldsymbol{z}^0)\big) \geq 2\ell+1 \quad (1 \leq s \leq n), \qquad \det Dg(\boldsymbol{z}^0) = J(\boldsymbol{x}^0, i_1, \ldots, i_n),$$

the first because replacing $\boldsymbol{y}^0$ by $\boldsymbol{y}$ changes each F_s by an element of $\varpi^{2\ell+1}\mathcal{O}_\wp$ (each x_i^s changes by a multiple of $\varpi^{2\ell+1}$), the second because $\partial F_s/\partial z_j = s\, z_j^{s-1}$ does not involve the free coordinates. These are the hypotheses of Greenberg's lemma over $\mathcal{O} = \mathcal{O}_\wp$, which produces $\boldsymbol{\zeta} = \boldsymbol{\zeta}(\boldsymbol{y}) \in \mathcal{O}_\wp^n$ with $g(\boldsymbol{\zeta}) = 0$, that is, $(\boldsymbol{\zeta}, \boldsymbol{y})$ is an exact solution of the system in $\mathcal{O}_\wp^k$.

Now let $h \geq 2\ell+1$. The number of residue classes of admissible $\boldsymbol{y}$ modulo ϖ^h is $N(\wp)^{(h-2\ell-1)(k-n)}$, and for every class the reduction of $(\boldsymbol{\zeta}(\boldsymbol{y}), \boldsymbol{y})$ modulo ϖ^h is a solution counted by $W(\wp^h, k)$. Distinct classes of $\boldsymbol{y}$ give solutions with distinct free components, hence distinct solutions. The bound follows. Moreover, $\boldsymbol{y} \equiv \boldsymbol{y}^0 \pmod{\varpi^{2\ell+1}}$ and Greenberg's lemma gives $\boldsymbol{\zeta}(\boldsymbol{y}) \equiv \boldsymbol{z}^0 \pmod{\varpi^{\ell+1}}$, so every solution constructed is congruent to $\boldsymbol{x}^0$ modulo $\varpi^{\ell+1}$. □

Lemma 4.28. *Let $k > n(n+1)$. If the system has a non-singular solution of level $\ell_\wp$ modulo $\wp^{2\ell_\wp+1}$, then*

$$\sigma_\wp \;\geq\; N(\wp)^{-(2\ell_\wp+1)(k-n)} \;>\; 0.$$

Proof. By Lemma 4.27, $W(\wp^h, k) \geq N(\wp)^{(h-2\ell_\wp-1)(k-n)} = N(\wp)^{-(2\ell_\wp+1)(k-n)}\, N(\wp)^{h(k-n)}$ for $h \geq 2\ell_\wp + 1$, and Lemma 4.25 gives $\sigma_\wp \geq N(\wp)^{-(2\ell_\wp+1)(k-n)}$. □

Lemma 4.29 (cf. [25, Theorem 6.1, p. 72])**.** *Let $n \geq 2$ and $k > n(n+1)$. There is $C = C(n, m, k)$ such that for every prime ideal $\wp$ with $N(\wp) > C$ the following hold.*

(i) $|\sigma_\wp - 1| \leq N(\wp)^{-1-\eta/2}$.

(ii) The system modulo $\wp$ has a non-singular solution of level 0.

Proof. (i) By the bound (4.6), which holds for every prime ideal $\wp$ and all exponents $e_1, \dots, e_n \geq 0$ with $\max_s e_s = l \geq 1$,

$$\begin{aligned} |\sigma_\wp - 1| &\leq \sum_{\substack{e_1,\dots,e_n \geq 0 \\ \max e_s = l \geq 1}} |A(\wp^{e_1}, \dots, \wp^{e_n})| \\ &\leq n^{(2m+1)k} \sum_{l \geq 1} (l+1)^n \, N(\wp)^{-l(1+\eta)} \;\ll_n\; n^{(2m+1)k} \, N(\wp)^{-1-\eta}, \end{aligned}$$

since the number of tuples $(e_1, \dots, e_n)$ with $\max e_s = l$ is at most $(l+1)^n$, $n - k/n = -1 - \eta$, and $\sum_{l \geq 1} (l+1)^n x^l \ll_n x$ for $0 < x \leq \frac{1}{2}$. The last bound is at most $N(\wp)^{-1-\eta/2}$ for $N(\wp) > C$.

(ii) By Theorem 4.24 with $\mathfrak{q} = \wp$, the same bound restricted to $e_s \in \{0, 1\}$ gives, for $N(\wp) > C$,

$$W(\wp, k) = N(\wp)^{k-n}\Big(1 + O\big(N(\wp)^{-1-\eta}\big)\Big) \;\geq\; \tfrac{1}{2} N(\wp)^{k-n}.$$

Enlarge C so that also $C > n^m$. Then the rational prime p below $\wp$ satisfies $p > n$ (since $N(\wp) = p^f$ with $f \leq m$), so $\wp \nmid n!$ and, by the Vandermonde formula in the definition of non-singularity, a solution is non-singular of level 0 if n of its coordinates are pairwise distinct modulo $\wp$. A solution without n pairwise distinct coordinates takes at most $n-1$ distinct values modulo $\wp$. The number of such k-tuples is at most $(n-1)^k N(\wp)^{n-1}$, which is less than $\frac{1}{4} N(\wp)^{k-n}$ for $N(\wp) > C$, since $k - n > n - 1$. Hence non-singular solutions of level 0 exist. Each condition imposed on C involves only n, m and k. □

Theorem 4.30. *Let $n \geq 2$ and $k > n(n+1)$, and let C be the constant of Lemma 4.29. Assume that, for every prime ideal $\wp$ with $N(\wp) \leq C$, there are $\ell_\wp \geq 0$ and a non-singular solution of level $\ell_\wp$ of*

$$x_1^s + \cdots + x_k^s \equiv N_s \pmod{\wp^{2\ell_\wp + 1}}, \qquad 1 \leq s \leq n.$$

Then

$$\sigma \;\geq\; c_1 \prod_{N(\wp) \leq C} N(\wp)^{-(2\ell_\wp+1)(k-n)} \;>\; 0, \qquad c_1 = \prod_{N(\wp) > C} \big(1 - N(\wp)^{-1-\eta/2}\big) > 0.$$

The constant C depends only on n, m and k, while $c_1 = c_1(K, n, k)$ depends on K, because the product defining it runs over the prime ideals of $\mathcal{O}_K$.

Proof. The proof follows Wang's argument for the single equation case [25, Theorem 6.1]. By Lemma 4.22, $\sigma = \prod_{\wp} \sigma_{\wp}$. For $N(\wp) > C$, Lemma 4.29(i) gives $\sigma_{\wp} \geq 1 - N(\wp)^{-1-\eta/2}$, and $\prod_{N(\wp)>C} \left(1 - N(\wp)^{-1-\eta/2}\right)$ converges to a positive number by comparison with $\zeta_K(1+\eta/2)^{-1}$ ($\zeta_K(u) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-u}$, the Dedekind zeta function of K, convergent for $u > 1$). For $N(\wp) \leq C$, Lemma 4.28 gives $\sigma_{\wp} \geq N(\wp)^{-(2\ell_{\wp}+1)(k-n)} > 0$. Multiplying the two bounds gives the theorem. $\square$

Chapter 5

The Quadratic Case for $p \leq n$

We consider quadratic fields first, because this special case illustrates the method in detail and shows how it generalizes to an arbitrary number field, which is the subject of Chapter 6.

Let C be the constant of Lemma 4.29. By Lemma 4.25 and Lemma 4.29(i), a positive lower bound for σ independent of $N_1, \ldots, N_n$ follows from lower bounds of the form

$$W(\wp^h, k) \geq c_\wp \, N(\wp)^{h(k-n)}, \qquad c_\wp > 0,$$

with $c_\wp$ independent of $N_1, \ldots, N_n$, for the finitely many prime ideals $\wp$ with $N(\wp) \leq C$.

For a prime ideal $\wp$ above a rational prime $p > n$, the solutions of the system modulo $\wp$ are counted by a character sum over $\mathcal{O}_K/\wp$ and lifted by Lemma 4.27, and Condition (M) of Definition 5.3 is not needed; Chapter 6 gives this argument for every number field (Theorem 6.5). For $p \leq n$, the number $n!$ lies in $\wp$, the standard (non-singular) form of Hensel's lemma does not apply, and the solutions are constructed from Condition (M) and lifted step by step. This chapter gives the construction for a quadratic field, and Chapter 6, for an arbitrary number field.

In this chapter, unless a lemma states otherwise, K is a quadratic field, $n \geq 3$, $k > n(n+1)$, and $p \leq n$.

5.1 Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 0, 1$ is a square-free integer. Let $\omega = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ and $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$. Then $\{1, \omega\}$ is an integral basis of K, and we use this

basis throughout the chapter. The minimal polynomial of ω is

$$\Phi = X^2 - d \quad \text{or} \quad \Phi = X^2 - X + \tfrac{1-d}{4}$$

in the two cases, and the discriminant of K is $\Delta_K = 4d$ or $\Delta_K = d$. See [15, Chapter 2].

The prime ideals of $\mathcal{O}_K$ fall into three kinds, which are determined by Φ. Here $\mathcal{O}_K = \mathbb{Z}[\omega]$, $\Phi \in \mathbb{Z}[X]$, and $\operatorname{disc}\Phi = \Delta_K$. For a rational prime p, let $\bar{\Phi}$ be the reduction of Φ modulo p.

Proposition 5.1. *Let p be a rational prime. Then exactly one of the following holds.*

(i) *$\bar{\Phi}$ has two distinct roots c, c' modulo p. Then $(p) = \wp\wp'$, where $\wp = (p, \omega - c)$ and $\wp' = (p, \omega - c')$ are distinct prime ideals of norm p, and $p \nmid \Delta_K$. We call $\wp$ and $\wp'$* split.

(ii) *$\bar{\Phi}$ has no root modulo p. Then $\wp = (p)$ is a prime ideal of norm p^2, and $p \nmid \Delta_K$. We call $\wp$* inert.

(iii) *$\bar{\Phi}$ has a double root c modulo p. Then $(p) = \wp^2$, where $\wp = (p, \omega - c)$ is a prime ideal of norm p, and $p \mid \Delta_K$. We call $\wp$* ramified.

Proof. See [15, Chapter 3, Theorems 25 and 27]. □

Every prime ideal of $\mathcal{O}_K$ lies above exactly one rational prime, so it is split, inert, or ramified.

5.2 The Arithmetic Condition

Condition (3.1) of Chapter 3 comes from Lemma 3.3, whose coefficients $\binom{x}{r}\binom{n-x}{n-r}$ are in general not algebraic integers for an algebraic integer x. In this section, we prove an analogue of Lemma 3.3 over $\mathbb{Z}[\omega]$ and state the arithmetic condition over K.

For $j \geq 0$, let

$$\binom{X}{j} = \frac{X(X-1)\cdots(X-j+1)}{j!} \in \mathbb{Q}[X], \qquad \binom{X}{0} = 1,$$

and for $0 \leq r \leq n$, set

$$t_r(X) = \binom{X}{r}\binom{n-X}{n-r}.$$

Then, for $0 \le j, r \le n$, we have $t_r(j) = 1$ if $j = r$ and $t_r(j) = 0$ if $j \ne r$. Indeed, if $j < r$, then $\binom{j}{r} = 0$. If $j > r$, then $\binom{n-j}{n-r} = 0$. Also, $t_r(r) = 1$. Hence, for $0 \le s \le n$, the polynomial $X^s - \sum_{r=0}^{n} r^s\, t_r(X)$ has degree at most n and vanishes at the $n+1$ points $0, 1, \ldots, n$, so it is the zero polynomial. Taking linear combinations, we obtain, for every polynomial $A \in \mathbb{Q}[X]$ of degree at most n,

$$A(X) = \sum_{r=0}^{n} A(r)\, t_r(X). \tag{5.1}$$

Both sides are linear in A and $t_r \in \mathbb{Q}[X]$, so (5.1) also holds for a polynomial A of degree at most n with coefficients in a number field K or in a polynomial ring $K[Y]$, and these are the cases used below. Moreover, $t_r(z)$ is an integer for every integer z, since both binomial coefficients are integers. For $z < 0$, this follows from the identity $\binom{z}{r} = (-1)^r \binom{r-z-1}{r}$, and for $z > n$ from $\binom{n-z}{n-r} = (-1)^{n-r}\binom{z-r-1}{n-r}$. For $0 \le z \le n$, both upper arguments are non-negative.

Now let z be an integer. Taking $A = X^s$ with $1 \le s \le n$ in (5.1) and evaluating at $X = z$, we obtain

$$\sum_{r=1}^{n} t_r(z)\, r^s = z^s, \qquad s = 1, \ldots, n,$$

since the term with $r = 0$ vanishes. Taking $A = 1$, we obtain

$$\sum_{r=0}^{n} t_r(z) = 1. \tag{5.2}$$

Lemma 5.2. *Let $n \ge 1$, let $\{1, \omega\}$ be an integral basis of the quadratic field K, and let $t_r(X)$, $0 \le r \le n$, be as above. Let $x = a + b\omega$ with $a, b \in \mathbb{Z}$, and let*

$$t_{r,l} = t_r(a)\, t_l(b), \qquad 0 \le r, l \le n.$$

Then $t_{r,l} \in \mathbb{Z}$,

$$\sum_{r=0}^{n} \sum_{l=0}^{n} t_{r,l}\, (r + l\omega)^s = x^s, \qquad s = 1, \ldots, n, \tag{5.3}$$

and $\sum_{r=0}^{n} \sum_{l=0}^{n} t_{r,l} = 1$. Moreover, the term with $(r, l) = (0, 0)$ in (5.3) is zero, so only the $(n+1)^2 - 1$ non-zero points $r + l\omega$ occur. These points are non-zero since 1 and ω are $\mathbb{Q}$-linearly independent.

Proof. Fix $1 \le s \le n$, and consider $(X + Y\omega)^s$ as a polynomial in X of degree $s \le n$ with coefficients in $K[Y]$. By (5.1),

$$(X + Y\omega)^s = \sum_{r=0}^{n} t_r(X)\,(r + Y\omega)^s.$$

Evaluating at $X = a$, we obtain

$$(a + Y\omega)^s = \sum_{r=0}^{n} t_r(a)\,(r + Y\omega)^s$$

in $K[Y]$. Each $(r+Y\omega)^s$ is a polynomial in Y of degree $s \le n$, so by (5.1) again, evaluating at $Y = b$,

$$(r + b\omega)^s = \sum_{l=0}^{n} t_l(b)\,(r + l\omega)^s.$$

Combining these results, we obtain (5.3). By (5.2),

$$\sum_{r=0}^{n}\sum_{l=0}^{n} t_{r,l} = \Big(\sum_{r=0}^{n} t_r(a)\Big)\Big(\sum_{l=0}^{n} t_l(b)\Big) = 1.$$

Also, the term with $(r, l) = (0, 0)$ is $t_{0,0} \cdot 0^s = 0$ for $s \ge 1$. □

Definition 5.3. Let $\Gamma_n(\mathcal{O}_K) \subseteq \mathcal{O}_K^n$ be the subgroup of $\mathcal{O}_K^n$ generated by the vectors $(x, x^2, \dots, x^n)$, $x \in \mathcal{O}_K$, that is, the set of all finite sums $\sum_i a_i(x_i, x_i^2, \dots, x_i^n)$ with $a_i \in \mathbb{Z}$ and $x_i \in \mathcal{O}_K$. We say that $N_1, \dots, N_n$ satisfy Condition (M) if $(N_1, \dots, N_n) \in \Gamma_n(\mathcal{O}_K)$.

Condition (M) is the arithmetic condition over K. For $K = \mathbb{Q}$, the group $\Gamma_n(\mathbb{Z})$ is generated by the n vectors $(r, r^2, \dots, r^n)$, $1 \le r \le n$ (Lemma 3.3), and Condition (M) is condition (3.1).

Lemma 5.4. *Let $n \ge 1$, and let $\{1, \omega\}$ be an integral basis of the quadratic field K.*

(i) $\Gamma_n(\mathcal{O}_K)$ is generated by the $(n+1)^2 - 1$ vectors $\big(r + l\omega, (r + l\omega)^2, \dots, (r + l\omega)^n\big)$ with $0 \le r, l \le n$, $(r, l) \ne (0, 0)$. Hence Condition (M) *of Definition 5.3 holds if and only if the system*

$$\sum_{\substack{0 \le r,l \le n \\ (r,l) \ne (0,0)}} t_{r,l}\,(r + l\omega)^s = N_s, \qquad s = 1, \dots, n,$$

has a solution in integers $t_{r,l}$.

(ii) If the system $x_1^s + \cdots + x_k^s = N_s$, $s = 1, \ldots, n$, has a solution with $x_1, \ldots, x_k \in \mathcal{O}_K$, then Condition (M) *holds. So Condition* (M) *is necessary for the solubility of the system.*

Proof. (i) The listed vectors are of the form $(x, x^2, \ldots, x^n)$, so they lie in $\Gamma_n(\mathcal{O}_K)$. Conversely, by Lemma 5.2, every vector $(x, x^2, \ldots, x^n)$ with $x \in \mathcal{O}_K$ is a $\mathbb{Z}$-linear combination of them.

(ii) We have $(N_1, \ldots, N_n) = \sum_{i=1}^k (x_i, x_i^2, \ldots, x_i^n) \in \Gamma_n(\mathcal{O}_K)$. □

5.3 Split Prime Ideals

Throughout this section, $\wp = (p, \omega - c)$ is a split prime ideal, as in Proposition 5.1(i), so that $(p) = \wp\wp'$ with $\wp' \neq \wp$, $N(\wp) = p$, and $p \nmid \Delta_K$.

Lemma 5.5. *Let $\wp = (p, \omega - c)$ be a split prime ideal of the quadratic field K, as in Proposition 5.1(i), and let $h \geq 1$. Then the following statements hold.*

(i) $\wp^h \cap \mathbb{Z} = p^h\mathbb{Z}$.

(ii) The reduction map $\phi_h \colon \mathbb{Z}/p^h\mathbb{Z} \to \mathcal{O}_K/\wp^h$ is a ring isomorphism.

(iii) There is an integer c_h, unique modulo p^h, such that $\omega \equiv c_h \pmod{\wp^h}$. It satisfies $\Phi(c_h) \equiv 0 \pmod{p^h}$ and $c_h \equiv c \pmod{p}$, and, for all integers a, b,

$$a + b\omega \equiv a + b\, c_h \pmod{\wp^h}.$$

Proof. (i) Since $p \in \wp$, we have $p^h \in \wp^h$, so $p^h\mathbb{Z} \subseteq \wp^h \cap \mathbb{Z}$. Conversely, let $0 \neq z \in \wp^h \cap \mathbb{Z}$, and write $z = p^j u$ with $p \nmid u$. The set $\wp \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ containing p, hence equal to $p\mathbb{Z}$. Thus $u \notin \wp$, and $v_\wp(u) = 0$. Since p is unramified and $\wp \mid (p)$, we have $v_\wp(p) = 1$, and hence $v_\wp(z) = j$. Now $z \in \wp^h$ means $v_\wp(z) \geq h$, so $j \geq h$ and $z \in p^h\mathbb{Z}$.

(ii) By (i), the composite map $\mathbb{Z} \to \mathcal{O}_K \to \mathcal{O}_K/\wp^h$ has kernel $p^h\mathbb{Z}$, so ϕ_h is an injective ring homomorphism. Both sides have p^h elements, since $|\mathcal{O}_K/\wp^h| = N(\wp)^h = p^h$. Hence ϕ_h is bijective.

(iii) Since ϕ_h is surjective, there is an integer c_h with $\omega \equiv c_h \pmod{\wp^h}$, and c_h is unique modulo p^h by (i) and (ii). Then $\Phi(c_h) \equiv \Phi(\omega) = 0 \pmod{\wp^h}$. Since $\Phi(c_h) \in \mathbb{Z}$, part (i) gives $\Phi(c_h) \equiv 0 \pmod{p^h}$. From $\omega \equiv c \pmod{\wp}$, we obtain $c_h - c \in \wp \cap \mathbb{Z} = p\mathbb{Z}$, and the last congruence follows. □

Recall from Definition 4.23 that, for $x_1, \dots, x_k$ running over a complete residue system modulo $\wp^h$, $W(\wp^h, k)$ is the number of solutions of

$$x_1^s + \cdots + x_k^s \equiv N_s \pmod{\wp^h}, \qquad s = 1, \dots, n,$$

and that $W(p^h, k)$ is the corresponding counting function of Chapter 3.

Lemma 5.6. *Let $n \geq 1$, $k \geq 1$, let $\wp = (p, \omega - c)$ be a split prime ideal of $\mathcal{O}_K$, as in Proposition 5.1(i), and let $N_1, \dots, N_n \in \mathcal{O}_K$. Let $h \geq 1$, and let c_h be as in Lemma 5.5. Write $N_s = a_s + b_s\omega$ with $a_s, b_s \in \mathbb{Z}$, and let $\tilde{N}_s = a_s + b_s c_h$, $s = 1, \dots, n$. Then*

$$W(\wp^h, k) = W(p^h, k),$$

where $W(p^h, k)$ is the counting function of Chapter 3 for the numbers $\tilde{N}_1, \dots, \tilde{N}_n$ in place of $N_1, \dots, N_n$.

Proof. Let $(x_1, \dots, x_k) \in (\mathcal{O}_K/\wp^h)^k$, and set $y_i = \phi_h^{-1}(x_i)$ for $i = 1, \dots, k$. Since ϕ_h^{-1} is a ring isomorphism, it preserves sums and products, so

$$\phi_h^{-1}\big(x_1^s + \cdots + x_k^s\big) = y_1^s + \cdots + y_k^s, \qquad s = 1, \dots, n,$$

and by Lemma 5.5(iii), we have $\phi_h^{-1}(N_s \bmod \wp^h) = \tilde{N}_s \bmod p^h$. Hence, for every s,

$$x_1^s + \cdots + x_k^s \equiv N_s \pmod{\wp^h} \qquad \Longleftrightarrow \qquad y_1^s + \cdots + y_k^s \equiv \tilde{N}_s \pmod{p^h}.$$

Therefore, $(x_1, \dots, x_k) \mapsto (y_1, \dots, y_k)$ is a bijection between the solutions of the two systems, with inverse induced by ϕ_h, and the two counting functions are equal. □

Lemma 5.7. *Let $n \geq 1$, and let $\wp = (p, \omega - c)$ be a split prime ideal of $\mathcal{O}_K$. Suppose that $N_1, \dots, N_n$ satisfy Condition* (M) *of Definition 5.3, and let h, c_h, $\tilde{N}_s$ be as in Lemma 5.6. Then there exist non-negative integers $\tilde{t}_1, \dots, \tilde{t}_n$ such that the natural numbers*

$$\hat{N}_s = \sum_{r=1}^{n} \tilde{t}_r \, r^s, \qquad s = 1, \dots, n,$$

satisfy

$$\hat{N}_s \equiv \tilde{N}_s \pmod{p^h}, \qquad s = 1, \dots, n.$$

In particular, $\hat{N}_1, \dots, \hat{N}_n$ satisfy condition (3.1).

Proof. By Condition (M), there are finitely many $x_i \in \mathcal{O}_K$ and $u_i \in \mathbb{Z}$ such that $N_s = \sum_i u_i\, x_i^s$ for $s = 1, \dots, n$. Let $y_i \in \mathbb{Z}$ be a representative of $\phi_h^{-1}(x_i \bmod \wp^h)$. Reducing modulo $\wp^h$ and applying ϕ_h^{-1}, we obtain

$$\tilde{N}_s \equiv \sum_i u_i\, y_i^s \pmod{p^h}, \qquad s = 1, \dots, n.$$

Taking $A = X^s$ in (5.1) and evaluating at $X = y_i$, we have, for $s = 1, \dots, n$,

$$y_i^s = \sum_{r=1}^{n} t_r(y_i)\, r^s,$$

since the term with $r = 0$ vanishes. Let $\tilde{t}'_r = \sum_i u_i\, t_r(y_i) \in \mathbb{Z}$. Combining these results, we obtain $\sum_{r=1}^n \tilde{t}'_r\, r^s \equiv \tilde{N}_s \pmod{p^h}$ for $s = 1, \dots, n$. Let $\tilde{t}_r = \tilde{t}'_r + p^h L$ for a positive integer L. This changes $\sum_r \tilde{t}_r\, r^s$ by $p^h L \sum_{r=1}^n r^s$, so the congruences are preserved, and for L large enough all $\tilde{t}_r$ are non-negative and all $\hat{N}_s$ are positive. □

Recall from Lemma 3.4 that, for a prime $p \le n$, $\varkappa$ is the integer with $p^\varkappa \le n < p^{\varkappa+1}$, $\delta = v_p\big((n-1)!\big)$, $k_1 = n^2 2^{2n-1}$, and $c_*^{\mathbb{Q}} = p^{(2\varkappa+2\delta+1)(n-k_1)}$.

Theorem 5.8. *Let $n \ge 3$, let $\wp = (p, \omega - c)$ be a split prime ideal, as in Proposition 5.1(i), with $p \le n$, and suppose that $N_1, \dots, N_n$ satisfy Condition* (M) *of Definition 5.3. Then, for $k \ge k_1 = n^2 2^{2n-1}$ and every $h \ge 1$,*

$$W(\wp^h, k) \;\ge\; c_*^{\mathbb{Q}}\, N(\wp)^{h(k-n)}, \qquad c_*^{\mathbb{Q}} = p^{(2\varkappa+2\delta+1)(n-k_1)}.$$

Hence $\sigma_\wp \ge c_*^{\mathbb{Q}} > 0$.

Proof. Let $h \ge 1$. By Lemma 5.6, $W(\wp^h, k)$ is the number of solutions of

$$y_1^s + \cdots + y_k^s \equiv \tilde{N}_s \pmod{p^h}, \qquad s = 1, \dots, n, \tag{5.4}$$

and $N(\wp)^{h(k-n)} = p^{h(k-n)}$. By Lemma 5.7, there are natural numbers $\hat{N}_1, \dots, \hat{N}_n$ satisfying condition (3.1) and $\hat{N}_s \equiv \tilde{N}_s \pmod{p^h}$. The number of solutions of (5.4) depends on $\tilde{N}_1, \dots, \tilde{N}_n$ only through their residues modulo p^h, so we may replace them by $\hat{N}_1, \dots, \hat{N}_n$. Since $p \le n$ and $k \ge k_1$, Lemma 3.4 gives $W(p^h, k) \ge c_*^{\mathbb{Q}}\, p^{h(k-n)}$. The constant does not depend on h, and $k \ge k_1 > n(n+1)$, so Lemma 4.25, applied with $h_\wp = 1$, gives $\sigma_\wp \ge c_*^{\mathbb{Q}}$. □

5.4 Auxiliary Lemmas

The lemmas of this section hold for every number field K and every prime ideal $\wp$ of $\mathcal{O}_K$. Throughout, $\wp$ lies above the rational prime p, $e = v_\wp(p)$ is its ramification index, and $N(\wp) = q = p^f$, where f is its residue degree. We fix $\varpi \in \wp \setminus \wp^2$, so that $v_\wp(\varpi) = 1$, and a complete residue system R modulo $\wp$. The set $\wp \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ containing p, hence equal to $p\mathbb{Z}$. If $z = p^j u$ is a non-zero integer with $p \nmid u$, then $u \notin \wp$, so $v_\wp(z) = ej$. That is, for every non-zero integer z,

$$v_\wp(z) = e\, v_p(z). \tag{5.5}$$

Recall from Definition 4.23 that $W(\wp^h, k)$ is the number of solutions of the system modulo $\wp^h$, and that it depends on $N_1, \ldots, N_n$. When $N_1', \ldots, N_n'$ take the place of $N_1, \ldots, N_n$ in the system, we write $W(\wp^h, k; N_1', \ldots, N_n')$.

Lemma 5.9. *Let K be a number field, and let $\wp$ be a prime ideal of $\mathcal{O}_K$. Let $\xi \in \mathcal{O}_K$ be non-zero, let $t = v_\wp(\xi)$, and let $u \geq 1$ be an integer. The map $y \mapsto \xi y$ induces a bijection from $\mathcal{O}_K/\wp^u$ onto $\wp^t/\wp^{t+u}$. In particular, every $x \in \mathcal{O}_K$ with $v_\wp(x) \geq t$ satisfies $x \equiv \xi y \pmod{\wp^{t+u}}$ for some $y \in \mathcal{O}_K$.*

Proof. The element ξy lies in $\wp^t$ because $v_\wp(\xi y) = t + v_\wp(y) \geq t$. For $y, y' \in \mathcal{O}_K$, we have $\xi y \equiv \xi y' \pmod{\wp^{t+u}}$ if and only if $v_\wp(y - y') \geq u$, that is, $y \equiv y' \pmod{\wp^u}$. Hence the map is well defined and injective. The reduction map $\mathcal{O}_K/\wp^{t+u} \to \mathcal{O}_K/\wp^t$ is surjective with kernel $\wp^t/\wp^{t+u}$, so

$$|\wp^t/\wp^{t+u}| = \frac{N(\wp)^{t+u}}{N(\wp)^t} = N(\wp)^u = |\mathcal{O}_K/\wp^u|,$$

and an injective map between finite sets with the same number of elements is bijective. The last statement is the surjectivity, applied to the class of x in $\wp^t/\wp^{t+u}$. □

Lemma 5.10. *Let K be a number field, and let $\wp$ be a prime ideal of $\mathcal{O}_K$ above the rational prime p, with $v_\wp(p) = e$. Let $\eta \in K$ with $v_\wp(\eta) \geq 0$, and let $u \geq 1$. Then there is $y \in \mathcal{O}_K$ with $v_\wp(y - \eta) \geq u$.*

Proof. Write the coordinates of η in the basis $\omega_1, \ldots, \omega_m$ as fractions, and let b_0 be a common denominator, so that $\eta = z b_0^{-1}$ with $z \in \mathcal{O}_K$ and a non-zero integer b_0. Write $b_0 = p^j b_1$ with $p \nmid b_1$. Then

$$v_\wp(z) = v_\wp(\eta) + v_\wp(b_0) \;\geq\; ej \;=\; v_\wp(p^j),$$

so Lemma 5.9, applied with $\xi = p^j$, gives $z' \in \mathcal{O}_K$ with $z \equiv p^j z' \pmod{\wp^{ej+u}}$. Also, $v_\wp(b_1) = e\, v_p(b_1) = 0$, so $b_1 \notin \wp$. Since $\wp/\wp^u$ is the unique maximal ideal of $\mathcal{O}_K/\wp^u$, the class of b_1 is invertible in this ring, and there is $b_1' \in \mathcal{O}_K$ with $b_1 b_1' \equiv 1 \pmod{\wp^u}$. Let $y = z' b_1' \in \mathcal{O}_K$. Then

$$y - \eta = z' b_1^{-1}\big(b_1 b_1' - 1\big) - \big(z - p^j z'\big)\, p^{-j} b_1^{-1},$$

and both terms have valuation at least u, the first because $v_\wp(z') \geq 0$ and $v_\wp(b_1) = 0$, and the second because $v_\wp(z - p^j z') \geq ej + u$. □

Lemma 5.11. *Let $n \geq 3$, and let $p \leq n$ be a prime. Let $\varkappa$ and δ be as in Lemma 3.4, that is, $p^\varkappa \leq n < p^{\varkappa+1}$ and $\delta = v_p\big((n-1)!\big)$. Then $p^{2\varkappa+2\delta+1} \leq n^2 2^{2n-1}$.*

Proof. Since $p^\varkappa \leq n$, we have $p^{2\varkappa} \leq n^2$, so it is enough to show $p^{2\delta+1} \leq 2^{2n-1}$. If $\delta = 0$, then $p^{2\delta+1} = p \leq n \leq 2^{2n-1}$. Suppose $\delta \geq 1$. Then $p \leq n-1$, because for $p = n$ the number n is prime and $\delta = v_p\big((n-1)!\big) = 0$. Let $t \geq 1$ be the integer with $p^t \leq n-1 < p^{t+1}$. Then

$$\delta = \sum_{i=1}^{t} \Big\lfloor \frac{n-1}{p^i} \Big\rfloor \;\leq\; (n-1) \sum_{i=1}^{t} p^{-i} = \frac{n-1}{p-1}\big(1 - p^{-t}\big) \;\leq\; \frac{n-1}{p-1}\Big(1 - \frac{1}{n-1}\Big) = \frac{n-2}{p-1},$$

and hence

$$p^{2\delta+1} \;\leq\; p^{2\delta+2} \;\leq\; p^{\,\frac{2(n-2)}{p-1}+2}.$$

For $p = 3$, the last bound equals $3^{\,(n-2)+2} = 3^n$, and $3^n < 2^{2n-1}$ for $n \geq 3$. For $p \neq 3$, we use $p^{1/(p-1)} \leq 2$ and $p^4 \leq 2^{2p}$. Since $2(n-2) - 2(p-1) \geq 0$, we obtain

$$p^{\,\frac{2(n-2)}{p-1}+2} = p^4 \left(p^{\frac{1}{p-1}}\right)^{2(n-2)-2(p-1)} \;\leq\; 2^{2p}\, 2^{\,2(n-2)-2(p-1)} = 2^{2n-2} < 2^{2n-1}.$$

□

Lemma 5.12. *Let K be a number field, let $\wp$ be a prime ideal of $\mathcal{O}_K$, and let $n \geq 1$. Let $h \geq 1$, $n \leq k_0 \leq k$, and $c_\wp > 0$. Let $\mathcal{S} \subseteq \mathcal{O}_K^n$ be a set with the following property: if $(N_1, \dots, N_n) \in \mathcal{S}$ and $x \in \mathcal{O}_K$, then $(N_1 - x, N_2 - x^2, \dots, N_n - x^n) \in \mathcal{S}$. Suppose that, for all $(N_1, \dots, N_n) \in \mathcal{S}$,*

$$W(\wp^h, k_0; N_1, \dots, N_n) \;\geq\; c_\wp\, N(\wp)^{h(k_0-n)}.$$

Then, for all $(N_1, \dots, N_n) \in \mathcal{S}$,

$$W(\wp^h, k; N_1, \dots, N_n) \;\geq\; c_\wp\, N(\wp)^{h(k-n)}.$$

Proof. Let $(N_1, \dots, N_n) \in \mathcal{S}$. Fix the residue classes of $x_{k_0+1}, \dots, x_k$ modulo $\wp^h$, with representatives in $\mathcal{O}_K$, and let $N'_s = N_s - \sum_{i=k_0+1}^{k} x_i^s$ for $s = 1, \dots, n$. Then $(N'_1, \dots, N'_n) \in \mathcal{S}$, by the property of $\mathcal{S}$ applied $k - k_0$ times. The solutions $(x_1, \dots, x_k)$ of the system modulo $\wp^h$ with the fixed residues in the last $k-k_0$ coordinates correspond to the solutions $(x_1, \dots, x_{k_0})$ of the system with $N'_1, \dots, N'_n$ in place of $N_1, \dots, N_n$, so their number is $W(\wp^h, k_0; N'_1, \dots, N'_n) \ge c_\wp\, N(\wp)^{h(k_0-n)}$. This bound does not depend on the fixed residues. Summing over the $N(\wp)^{h(k-k_0)}$ choices of the residues, we obtain

$$W(\wp^h, k; N_1, \dots, N_n) \;\ge\; N(\wp)^{h(k-k_0)}\, c_\wp\, N(\wp)^{h(k_0-n)} \;=\; c_\wp\, N(\wp)^{h(k-n)}.$$

□

The set $\mathcal{S} = \mathcal{O}_K^n$ has the property required in Lemma 5.12, and so does every subgroup of $\mathcal{O}_K^n$ that contains the vectors $(x, x^2, \dots, x^n)$, $x \in \mathcal{O}_K$.

5.5 Inert and Ramified Prime Ideals

Throughout this section, $\wp$ is an inert or a ramified prime ideal of $\mathcal{O}_K$, as in Proposition 5.1(ii) or (iii), above a rational prime $p \le n$, and $e = v_\wp(p)$, the uniformizer ϖ and the complete residue system R modulo $\wp$ are as in Section 5.4. If $\wp = (p)$ is inert, then $N(\wp) = p^2$, $e = 1$, $\wp^h = p^h\mathcal{O}_K$ for every $h \ge 1$, and we may take $\varpi = p$ and for R the elements of $\mathcal{O}_K$ whose two coordinates in the basis $\{1, \omega\}$ lie in $\{0, 1, \dots, p-1\}$. If $\wp$ is ramified, then $(p) = \wp^2$, $N(\wp) = p$ and $e = 2$, and we may take for R the numbers $0, 1, \dots, p-1$, because the natural map $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\wp$ is injective and both rings have p elements. In both cases, $v_\wp(z) = e\, v_p(z)$ for every non-zero integer z, by (5.5). The reduction $\mathbb{Z} \to \mathcal{O}_K/\wp^h$ is not surjective for $h \ge 2$: in the inert case its image has at most p^h of the p^{2h} elements, and in the ramified case $p \in \wp^2$, so its image in $\mathcal{O}_K/\wp^2$ has p elements. Hence there is no isomorphism like ϕ_h, and we work directly in $\mathcal{O}_K$, with the powers of ϖ in place of the powers of p, following the method of Lemma 3.4, that is, of [3, Lemma 8.3, p. 321].

Recall from Lemma 3.4 that $p^\varkappa \le n < p^{\varkappa+1}$ and $\delta = v_p\big((n-1)!\big)$. We need two natural numbers α and β such that

$$\text{(i) } 2 \le \beta \le \alpha, \;\; \text{(ii) } 2\beta \ge \alpha+1, \;\; \text{(iii) } \beta > e\varkappa, \;\; \text{(iv) } \alpha-\beta = (\varkappa+\delta)e, \;\; \text{(v) } \beta+e\delta \le \alpha. \tag{5.6}$$

From now on, we take

$$\alpha = 2(\varkappa+\delta)e + 1, \qquad \beta = (\varkappa+\delta)e + 1, \tag{5.7}$$

so that $\alpha - \beta = (\varkappa + \delta)e$. Conditions (ii) and (iv) are clear. Condition (i) holds because $\varkappa \geq 1$ for $p \leq n$. Condition (iii) holds because $\beta > (\varkappa + \delta)e \geq e\varkappa$. Condition (v) says $e\delta \leq (\varkappa + \delta)e$, which is true. We also write

$$\alpha_0 = 2\varkappa + 2\delta + 1$$

for the value of α for $e = 1$. Then $\alpha \leq e\alpha_0$. For an inert prime ideal, $\alpha = \alpha_0$ and $\beta = \varkappa + \delta + 1$.

Lemma 5.13. *Let $n \geq 3$, let $\wp$ be an inert or a ramified prime ideal of the quadratic field K above the rational prime $p \leq n$, let $e = v_\wp(p)$, let $\varkappa$ and δ be as in Lemma 3.4, and let β be as in* (5.7)*. Let $x_1, \ldots, x_n \in \mathcal{O}_K$ satisfy $x_i \equiv i \pmod{\wp^\beta}$ for $1 \leq i \leq n$. For $1 \leq r \leq n$, write*

$$\Lambda_r(X) = \prod_{\substack{1 \leq i \leq n \\ i \neq r}} \frac{X - x_i}{x_r - x_i} = \sum_{s=1}^{n} \lambda(r,s)\, X^{s-1} \in K[X];$$

the numbers $x_1, \ldots, x_n$ are pairwise distinct by (i) below, so Λ_r is well defined. Then the following statements hold.

(i) For $i \neq r$, we have $v_\wp(x_r - x_i) = e\, v_p(r-i)$, and

$$v_\wp\Big(\prod_{i \neq r}(x_r - x_i)\Big) = e\, v_p\big((r-1)!\,(n-r)!\big) \leq e\delta.$$

(ii) $v_\wp\big(\lambda(r,s)\big) \geq -e\delta$ for all r and s.

(iii) $v_\wp\big(\Lambda_r(x)\big) \geq -e\delta$ for every $x \in \mathcal{O}_K$.

(iv) For $1 \leq s \leq n$,

$$X^{s-1} = \sum_{r=1}^{n} x_r^{s-1} \Lambda_r(X),$$

and hence $\sum_{r=1}^{n} x_r^{s-1} \lambda(r,t)$ equals 1 for $t = s$ and equals 0 for $t \neq s$.

Proof. (i) We have $x_r - x_i - (r-i) \in \wp^\beta$, so $v_\wp\big(x_r - x_i - (r-i)\big) \geq \beta$. We have $0 < |r-i| \leq n - 1 < p^{\varkappa+1}$ by the definition of $\varkappa$, so $v_p(r-i) \leq \varkappa$, and (5.5) and (5.6)(iii) give $v_\wp(r-i) = e\, v_p(r-i) \leq e\varkappa < \beta$. The two terms $r-i$ and $x_r - x_i - (r-i)$ have different valuations, so $v_\wp(x_r - x_i) = e\, v_p(r-i)$. Summing over $i \neq r$, we obtain

$e\,v_p\big(\prod_{i<r}(r-i)\prod_{i>r}(i-r)\big) = e\,v_p\big((r-1)!\,(n-r)!\big)$. Since $\binom{n-1}{r-1}$ is an integer, $(r-1)!\,(n-r)!$ divides $(n-1)!$, and the valuation is at most $e\,v_p\big((n-1)!\big) = e\delta$.

(ii) Expand the product $\prod_{i\neq r}(X-x_i)$. Each coefficient of the resulting polynomial is, up to sign, a sum of products of the numbers x_i, so it lies in $\mathcal{O}_K$. Each $\lambda(r,s)$ is such a coefficient divided by $\prod_{i\neq r}(x_r-x_i)$, so (i) gives $v_\wp(\lambda(r,s)) \geq -e\delta$.

(iii) For $x \in \mathcal{O}_K$, the product $\prod_{i\neq r}(x-x_i)$ lies in $\mathcal{O}_K$, and we divide by $\prod_{i\neq r}(x_r-x_i)$ as in (ii).

(iv) By (i), the numbers $x_1,\dots,x_n$ are pairwise distinct. Also, $\Lambda_r(x_j)$ equals 1 for $j=r$ and equals 0 for $j\neq r$. Hence the polynomial $X^{s-1} - \sum_{r=1}^n x_r^{s-1}\Lambda_r(X)$ has degree at most $n-1$ and vanishes at the n points $x_1,\dots,x_n$, so it is the zero polynomial. The second statement follows by comparing the coefficients of X^{t-1} on both sides. □

Lemma 5.14. *Let $n \geq 3$, let $\wp$ be an inert or a ramified prime ideal of the quadratic field K above the rational prime $p \leq n$, let $e = v_\wp(p)$ and $\varpi \in \wp \setminus \wp^2$, let $N_1,\dots,N_n \in \mathcal{O}_K$, let $k \geq n$, let $\varkappa$ and δ be as in Lemma 3.4, and let α, β be as in* (5.7). *Let $j \geq 0$, and write $\alpha_j = \alpha + j$ and $\beta_j = \beta + j$. Suppose that $(x_1,\dots,x_k) \in \mathcal{O}_K^k$ satisfies*

$$\sum_{i=1}^k x_i^s \equiv N_s \pmod{\wp^{\alpha_j}} \quad (1 \leq s \leq n), \qquad x_i \equiv i \pmod{\wp^\beta} \quad (1 \leq i \leq n).$$

Then for arbitrary $y_{n+1},\dots,y_k \in \mathcal{O}_K$ there exist $y_1,\dots,y_n \in \mathcal{O}_K$ such that the numbers

$$z_i = x_i + \varpi^{\beta_j} y_i \ (1 \leq i \leq n), \qquad z_i = x_i + \varpi^{\beta_j + e\delta} y_i \ (n < i \leq k)$$

satisfy

$$\sum_{i=1}^k z_i^s \equiv N_s \pmod{\wp^{\alpha_j+1}} \quad (1 \leq s \leq n), \qquad z_i \equiv i \pmod{\wp^\beta} \quad (1 \leq i \leq n).$$

Proof. We have $v_\wp(z_i - x_i) \geq \beta_j$ for every i. By (5.6)(ii), we have $2\beta_j = 2\beta + 2j \geq \alpha + 1 + 2j \geq \alpha_j + 1$, so every term of the expansion of $z_i^s = \big(x_i + (z_i - x_i)\big)^s$ that contains $(z_i - x_i)^2$ lies in $\wp^{\alpha_j+1}$. Hence

$$z_i^s \equiv x_i^s + s\,x_i^{s-1}(z_i - x_i) \pmod{\wp^{\alpha_j+1}}.$$

Since $v_\wp\big(N_s - \sum_{i=1}^k x_i^s\big) \geq \alpha_j$, Lemma 5.9, applied with $\xi = \varpi^{\alpha_j}$ and $u = 1$, gives $w_s \in \mathcal{O}_K$ with

$$N_s - \sum_{i=1}^k x_i^s \equiv \varpi^{\alpha_j} w_s \pmod{\wp^{\alpha_j+1}}.$$

Summing the congruences above over i, we see that $\sum_i z_i^s \equiv N_s \pmod{\wp^{\alpha_j+1}}$ holds for $s = 1, \ldots, n$ if and only if

$$\varpi^{\beta_j}\Big(\sum_{i=1}^{n} s\, x_i^{s-1} y_i + \varpi^{e\delta} \sum_{i=n+1}^{k} s\, x_i^{s-1} y_i\Big) \equiv \varpi^{\alpha_j} w_s \pmod{\wp^{\alpha_j+1}}, \qquad s = 1, \ldots, n.$$

For $z, z' \in \mathcal{O}_K$, we have $\varpi^{\beta_j} z \equiv \varpi^{\beta_j} z' \pmod{\wp^{\alpha_j+1}}$ if and only if $v_\wp(z - z') \geq \alpha_j + 1 - \beta_j$, by comparing valuations. Since $\alpha_j - \beta_j = \alpha - \beta = (\varkappa + \delta)e$, the congruences above can therefore be rewritten as

$$\sum_{i=1}^{n} s\, x_i^{s-1} y_i \;\equiv\; \varpi^{(\varkappa+\delta)e} w_s - \varpi^{e\delta} \sum_{i=n+1}^{k} s\, x_i^{s-1} y_i \pmod{\wp^{(\varkappa+\delta)e+1}}, \qquad s = 1, \ldots, n. \tag{5.8}$$

So it suffices to find $y_1, \ldots, y_n \in \mathcal{O}_K$ satisfying (5.8).

Let Λ_r and $\lambda(r,t)$ be as defined in Lemma 5.13 for $x_1, \ldots, x_n$, and let

$$\eta_r \;=\; \varpi^{(\varkappa+\delta)e} \sum_{t=1}^{n} t^{-1} \lambda(r,t)\, w_t \;-\; \varpi^{e\delta} \sum_{i=n+1}^{k} y_i\, \Lambda_r(x_i), \qquad r = 1, \ldots, n. \tag{5.9}$$

We show that

$$\sum_{i=1}^{n} s\, x_i^{s-1} \eta_i \;=\; \varpi^{(\varkappa+\delta)e} w_s - \varpi^{e\delta} \sum_{i=n+1}^{k} s\, x_i^{s-1} y_i, \qquad s = 1, \ldots, n.$$

Fix s and substitute (5.9) into the left-hand side. By Lemma 5.13(iv), the sum $\sum_{i=1}^{n} x_i^{s-1} \lambda(i,t)$ equals 1 for $t = s$ and 0 otherwise, so the terms arising from the first sum in (5.9) add up to $\varpi^{(\varkappa+\delta)e} s\, s^{-1} w_s = \varpi^{(\varkappa+\delta)e} w_s$. Taking $X = x_i$ in the identity of Lemma 5.13(iv), we obtain

$$\sum_{r=1}^{n} x_r^{s-1} \Lambda_r(x_i) = x_i^{s-1},$$

so the terms arising from the second sum add up to $-\varpi^{e\delta} \sum_{i=n+1}^{k} s\, x_i^{s-1} y_i$. This proves the claim.

We show that $v_\wp(\eta_r) \geq 0$. For the terms in the second sum of (5.9), Lemma 5.13(iii) gives

$$v_\wp\big(\varpi^{e\delta} y_i \Lambda_r(x_i)\big) \;\geq\; e\delta - e\delta = 0.$$

For the terms in the first sum, we have $v_\wp(t^{-1}) = -e\,v_p(t) \ge -e\varkappa$ by (5.5), because $t \le n < p^{\varkappa+1}$, so Lemma 5.13(ii) gives

$$v_\wp\big(\varpi^{\,(\varkappa+\delta)e} t^{-1}\lambda(r,t)w_t\big) \;\ge\; (\varkappa+\delta)e - e\varkappa - e\delta \;=\; 0.$$

By Lemma 5.10, applied with $u = (\varkappa+\delta)e+1$, there are $y_r \in \mathcal{O}_K$ with $v_\wp(y_r - \eta_r) \ge (\varkappa+\delta)e+1$ for $r = 1, \dots, n$. Hence

$$\sum_{i=1}^{n} s\,x_i^{s-1}y_i - \varpi^{\,(\varkappa+\delta)e} w_s + \varpi^{\,e\delta} \sum_{i=n+1}^{k} s\,x_i^{s-1}y_i = \sum_{i=1}^{n} s\,x_i^{s-1}(y_i - \eta_i)$$

also has valuation at least $(\varkappa+\delta)e+1$. This proves (5.8). The congruence $z_i \equiv i \pmod{\wp^\beta}$ holds because $\beta_j \ge \beta$. □

Lemma 5.15. *Let $n \ge 3$, let $\wp$ be an inert or a ramified prime ideal of the quadratic field K above the rational prime $p \le n$, let $N_1, \dots, N_n \in \mathcal{O}_K$, let $k \ge n$, and let α, β be as in (5.7). Suppose that $\big(x_i^{(0)}\big)_{1\le i\le k} \in \mathcal{O}_K^k$ satisfies*

$$\sum_{i=1}^{k} \big(x_i^{(0)}\big)^s \equiv N_s \pmod{\wp^\alpha} \quad (1 \le s \le n), \qquad x_i^{(0)} \equiv i \pmod{\wp^\beta} \quad (1 \le i \le n).$$

Then $W(\wp^h, k) \ge N(\wp)^{(h-\alpha)(k-n)}$ for every $h \ge \alpha$.

Proof. Let $L = h - \alpha$, and consider the matrices $\mathcal{Y} = \big(y_i^{(j)}\big)$ with $n < i \le k$ and $0 \le j < L$, whose entries lie in R. There are $N(\wp)^{(k-n)L}$ such matrices. We construct a solution modulo $\wp^h$ for every $\mathcal{Y}$. Starting from $\big(x_i^{(0)}\big)$, we apply Lemma 5.14 at the stages $j = 0, 1, \dots, L-1$. At stage j, we take $y_i^{(j)}$ for the free numbers y_i with $i > n$, and we fix one choice of the numbers $y_1, \dots, y_n$ given by the lemma. The assumptions of the lemma hold at every stage, since the modulus rises by one and the congruences $x_i \equiv i \pmod{\wp^\beta}$ still hold. After L stages, we obtain a solution of the system modulo $\wp^h$, and its coordinates with index $i > n$ are

$$z_i(\mathcal{Y}) = x_i^{(0)} + \varpi^{\,\beta+e\delta} \sum_{j=0}^{L-1} \varpi^{\,j}\, y_i^{(j)}.$$

Suppose $\mathcal{Y} \ne \mathcal{Y}'$. Choose $i > n$ and the smallest j with $y_i^{(j)} \ne y_i'^{(j)}$. Distinct elements of R are incongruent modulo $\wp$, so

$$v_\wp\big(z_i(\mathcal{Y}) - z_i(\mathcal{Y}')\big) = \beta + e\delta + j \;\le\; \beta + e\delta + L - 1 \;<\; \alpha + L = h,$$

where the last inequality follows from (5.6)(v). Hence the solutions constructed from $\mathcal{Y}$ and from $\mathcal{Y}'$ are incongruent modulo $\wp^h$, and the $N(\wp)^{(k-n)L}$ matrices give that many distinct solutions modulo $\wp^h$. □

Below, G denotes the set of the numbers $r + l\omega$ with $0 \le r, l \le n$ and $(r, l) \ne (0, 0)$. This is the set of points in Lemma 5.4(i), and it has $(n+1)^2 - 1$ elements.

Proposition 5.16. *Let $n \ge 3$, let $\wp$ be an inert or a ramified prime ideal of $\mathcal{O}_K$ above the rational prime $p \le n$, and suppose that $N_1, \dots, N_n$ satisfy Condition* (M) *of Definition 5.3. Let α be as in* (5.7)*, let $\alpha_0 = 2\varkappa + 2\delta + 1$, and set*

$$k_0 \;=\; n + \big((n+1)^2 - 1\big)\big(p^{\alpha_0} - 1\big).$$

Then, for every $k \ge k_0$ and every $h \ge 1$,

$$W(\wp^h, k) \;\ge\; N(\wp)^{\alpha(n-k_0)}\, N(\wp)^{h(k-n)}.$$

Proof. Let $k = k_0$. The vectors $(r, r^2, \dots, r^n)$ with $1 \le r \le n$ lie in $\Gamma_n(\mathcal{O}_K)$, so Condition (M) and Lemma 5.4(i) give integers t_g for $g \in G$ with

$$\sum_{g \in G} t_g\, g^s = N_s - (1^s + \cdots + n^s), \qquad s = 1, \dots, n.$$

Let u_g be the least non-negative residue of t_g modulo p^{α_0}, so that $0 \le u_g \le p^{\alpha_0} - 1$. Since $v_\wp(p^{\alpha_0}) = e\alpha_0 \ge \alpha$, we have $p^{\alpha_0}\mathcal{O}_K \subseteq \wp^\alpha$, so replacing each t_g by u_g changes the left-hand side only by an element of $\wp^\alpha$, and therefore

$$1^s + \cdots + n^s + \sum_{g \in G} u_g\, g^s \;\equiv\; N_s \pmod{\wp^\alpha}, \qquad s = 1, \dots, n.$$

We have $n + \sum_g u_g \le n + \big((n+1)^2 - 1\big)(p^{\alpha_0} - 1) = k_0$. Hence the tuple whose first n entries are $1, 2, \dots, n$, followed by u_g copies of each $g \in G$ and then by zeros, is a solution of the system modulo $\wp^\alpha$ with k_0 entries, and its first n entries satisfy $x_i = i$. For $h \ge \alpha$, Lemma 5.15 gives $W(\wp^h, k_0) \ge N(\wp)^{(h-\alpha)(k_0-n)}$. For $1 \le h < \alpha$, the reduction of this solution modulo $\wp^h$ shows $W(\wp^h, k_0) \ge 1$, and $1 \ge N(\wp)^{(h-\alpha)(k_0-n)}$ because $h < \alpha$ and $k_0 > n$. Hence, for all $h \ge 1$,

$$W(\wp^h, k_0) \;\ge\; N(\wp)^{(h-\alpha)(k_0-n)} \;=\; N(\wp)^{\alpha(n-k_0)}\, N(\wp)^{h(k_0-n)}. \tag{5.10}$$

The construction above used only Condition (M), so (5.10) holds for all $N_1, \dots, N_n$ satisfying (M), and Lemma 5.12, applied with $\mathcal{S} = \Gamma_n(\mathcal{O}_K)$, gives the bound for all $k \ge k_0$. □

Theorem 5.17. *Let $n \geq 3$, let $\wp$ be an inert or a ramified prime ideal of $\mathcal{O}_K$, as in Proposition 5.1(ii) or (iii), above a rational prime $p \leq n$, and suppose that $N_1, \ldots, N_n$ satisfy Condition* (M) *of Definition 5.3. Let $k_1' = (n+1)^2 n^2 2^{2n-1}$. Then, for $k \geq k_1'$ and every $h \geq 1$,*

$$W(\wp^h, k) \;\geq\; c_*' \, N(\wp)^{h(k-n)}, \qquad c_*' = \left(n^2 2^{2n-1}\right)^{2(n-k_1')}.$$

Hence $\sigma_\wp \geq c_*' > 0$.

Proof. Let α_0 and k_0 be as in Proposition 5.16. By Lemma 5.11, $p^{\alpha_0} \leq n^2 2^{2n-1}$. Hence

$$k_0 \;\leq\; n + \left((n+1)^2 - 1\right) n^2 2^{2n-1} \;\leq\; (n+1)^2 n^2 2^{2n-1} \;=\; k_1',$$

using $n \leq n^2 2^{2n-1}$. Also, $N(\wp)^\alpha \leq p^{2\alpha_0}$, because $N(\wp) = p^2$ and $\alpha = \alpha_0$ for an inert prime ideal, and $N(\wp) = p$ and $\alpha = 2\alpha_0 - 1$ for a ramified prime ideal. Hence

$$N(\wp)^\alpha \;\leq\; p^{2\alpha_0} \;\leq\; \left(n^2 2^{2n-1}\right)^2.$$

For $k \geq k_1'$, we therefore have

$$N(\wp)^{\alpha(n-k_0)} \;\geq\; N(\wp)^{\alpha(n-k_1')} \;\geq\; \left(n^2 2^{2n-1}\right)^{2(n-k_1')} \;=\; c_*',$$

and Proposition 5.16 gives $W(\wp^h, k) \geq c_*' \, N(\wp)^{h(k-n)}$. The constant c_*' does not depend on h, and $k \geq k_1' > n(n+1)$. Hence Lemma 4.25, applied with $h_\wp = 1$, gives $\sigma_\wp \geq c_*'$. $\square$

Chapter 6

The General Case

In this chapter, K is a number field of degree m, $\mathcal{O}_K$ its ring of integers, and $\omega_1, \dots, \omega_m$ an integral basis, as in Chapter 4. For a prime ideal $\wp$ above the rational prime p, let e be the ramification index and f the residue degree of $\wp$, so that $v_\wp(p) = e$, $N(\wp) = p^f$, and $ef \le m$ [13, Chapter I]. As in Chapter 5, our goal is lower bounds of the form $W(\wp^h, k) \ge c_\wp N(\wp)^{h(k-n)}$ with $c_\wp > 0$ independent of $N_1, \dots, N_n$, which by Lemma 4.25 give $\sigma_\wp \ge c_\wp$. In this chapter, unless a lemma states otherwise, $n \ge 3$ and $k > n(n+1)$.

6.1 Prime Ideals above $p > n$

In this section, $\wp$ is a prime ideal of $\mathcal{O}_K$ above a rational prime $p > n$, with $N(\wp) = q = p^f$. Recall from Section 5.4 that R is a complete residue system modulo $\wp$ and that $W(\wp^h, k; N_1', \dots, N_n')$ is the counting function with $N_1', \dots, N_n'$ in place of $N_1, \dots, N_n$. Write $F = \mathcal{O}_K/\wp$, a finite field with q elements.

Lemma 6.1. *Let $n \ge 1$, and let F be a finite field with q elements whose characteristic p satisfies $p > n$. Let $k \ge 1$ and $\nu_1, \dots, \nu_n \in F$, and let T be the number of $(x_1, \dots, x_k) \in F^k$ with*

$$x_1^s + \cdots + x_k^s = \nu_s, \qquad s = 1, \dots, n.$$

Then $\left|T - q^{k-n}\right| \le (nq^{1/2})^k$.

Proof. Let χ be a non-trivial additive character of F. For $u \in F$, the sum $\sum_{a \in F} \chi(au)$

equals q if $u = 0$ and equals 0 otherwise (see [14, Chapter 5]). Hence

$$T = q^{-n} \sum_{a_1 \in F} \cdots \sum_{a_n \in F} S(a_1, \ldots, a_n)^k \, \chi\big(- a_1\nu_1 - \cdots - a_n\nu_n\big),$$

where

$$S(a_1, \ldots, a_n) = \sum_{x \in F} \chi\big(a_1 x + a_2 x^2 + \cdots + a_n x^n\big).$$

The term with $a_1 = \cdots = a_n = 0$ equals q^{k-n}. Suppose $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$. Then the polynomial $a_1 X + \cdots + a_n X^n$ has degree d for some $1 \le d \le n$, and d is not divisible by p because $p > n \ge d$. Hence Weil's bound [14, Theorem 5.38] gives $|S(a_1, \ldots, a_n)| \le (d-1)q^{1/2} \le nq^{1/2}$. There are fewer than q^n such terms, so the total error is at most $q^{-n} \cdot q^n \, (nq^{1/2})^k = (nq^{1/2})^k$. □

Lemma 6.2. *Let $n \ge 3$, and let q and k be real numbers with $q \ge 9n^2$ and $k \ge 6n^2$. Then*

$$n^k q^{n-k/2} \;\le\; q^{-4} \qquad \textit{and} \qquad q^{n-1} n^k \;\le\; q^{k-n-4}.$$

Proof. Suppose first that $q \ge n^3$. Then $n^k \le q^{k/3}$, so

$$n^k q^{n-k/2} \;\le\; q^{n-k/6} \;\le\; q^{n-n^2} \;\le\; q^{-6},$$

because $k \ge 6n^2$ and $n \ge 3$. Suppose next that $q < n^3$. From $9n^2 \le q < n^3$, we obtain $n > 9$. Also, $nq^{-1/2} \le 1/3$, so

$$n^k q^{n-k/2} = q^n \big(nq^{-1/2}\big)^k \;\le\; n^{3n}\, 3^{-6n^2}.$$

Since $n \le 3^n$, we have $n^{3n} 3^{-6n^2} \le \big(3^n 3^{-2n}\big)^{3n} = 3^{-3n^2}$, and also $n^{12} \le 3^{12n} \le 3^{3n^2}$ because $12n \le 3n^2$ for $n \ge 4$. Hence

$$n^k q^{n-k/2} \;\le\; 3^{-3n^2} \;\le\; n^{-12} \;<\; q^{-4},$$

where the last step uses $q < n^3$. This proves the first inequality. For the second, we have

$$q^{n-1} n^k \;=\; q^{k-n} \cdot n^k q^{2n-1-k} \;\le\; q^{k-n} \cdot n^k q^{n-k/2} \;\le\; q^{k-n-4},$$

where the first inequality uses $2n - 1 - k \le n - k/2$, which holds because $k \ge 2n - 2$. □

Lemma 6.3. *Let $n \ge 1$, let $\wp$ be a prime ideal of the number field K above the rational prime p, with $q = N(\wp)$, and let $N_1, \ldots, N_n \in \mathcal{O}_K$. Let $p > n$ and $k \ge n$. Let W_1 be the number of solutions of the system modulo $\wp$, with $x_1, \ldots, x_k$ in a complete residue system modulo $\wp$, in which some n of the coordinates are pairwise incongruent modulo $\wp$. Then the following statements hold.*

(i) $W_1 \;\geq\; W(\wp, k) - q^{\,n-1} n^k$.

(ii) $W(\wp^h, k) \;\geq\; q^{\,(h-1)(k-n)}\, W_1$ *for every* $h \geq 1$.

Proof. (i) A solution modulo $\wp$ that is not counted by W_1 has all its coordinates in a set of at most $n-1$ residue classes modulo $\wp$. The number of k-tuples of this kind is at most $\binom{q}{n-1}(n-1)^k \leq q^{\,n-1} n^k$.

(ii) Let $\boldsymbol{x} = (x_1, \ldots, x_k)$ be counted by W_1, and choose indices $i_1 < \cdots < i_n$ such that $x_{i_1}, \ldots, x_{i_n}$ are pairwise incongruent modulo $\wp$. In the notation of Definition 4.26,

$$J(\boldsymbol{x}, i_1, \ldots, i_n) = n! \prod_{1 \leq j < j' \leq n} \left(x_{i_{j'}} - x_{i_j} \right)$$

lies outside $\wp$, because $v_\wp(n!) = e\, v_p(n!) = 0$ for $p > n$ and each factor $x_{i_{j'}} - x_{i_j}$ lies outside $\wp$. Hence $\boldsymbol{x}$ is a non-singular solution of level 0 modulo $\wp$, and Lemma 4.27, applied with $\ell = 0$, so that $h \geq 1 = 2\ell + 1$, gives at least $q^{\,(h-1)(k-n)}$ solutions modulo $\wp^h$ that are congruent to $\boldsymbol{x}$ modulo $\wp$. Solutions obtained from two different $\boldsymbol{x}$ are incongruent modulo $\wp$, hence incongruent modulo $\wp^h$. Summing over the W_1 solutions $\boldsymbol{x}$ gives (ii). □

Lemma 6.4. *Let $n \geq 3$, let $\wp$ be a prime ideal of the number field K above the rational prime p, and let $N_1, \ldots, N_n \in \mathcal{O}_K$. Let $p > n$, and let $k_2 = \lfloor 32n^2 \ln n \rfloor + n$ be as in Lemma 3.7. Suppose that $k \geq k_2$. Then the system modulo $\wp$ has a solution with $x_i \equiv i \pmod{\wp}$ for $1 \leq i \leq n$. In particular, the number W_1 of Lemma 6.3 satisfies $W_1 \geq 1$.*

Proof. Since $p > n$, the integers $1, \ldots, n$ are pairwise incongruent modulo $\wp$, so a solution with $x_i \equiv i$ for $1 \leq i \leq n$ is counted by W_1. Such a solution exists if and only if the system

$$x_{n+1}^s + \cdots + x_k^s = \nu_s, \qquad s = 1, \ldots, n, \tag{6.1}$$

has a solution in $F^{\,k-n}$, where ν_s is the class of $N_s - (1^s + \cdots + n^s)$ modulo $\wp$.

Suppose first that $q = p$. The natural map $\mathbb{Z}/p\mathbb{Z} \to F$ is an isomorphism, because $\wp \cap \mathbb{Z} = p\mathbb{Z}$ and both rings have p elements. Hence the number of solutions of (6.1) is the number T_1 of Chapter 3, with $k - n \geq \lfloor 32n^2 \ln n \rfloor$ variables and with integer representatives of $\nu_1, \ldots, \nu_n$ in place of $N_1, \ldots, N_n$. Since $\lfloor 32n^2 \ln n \rfloor \geq 4n \ln n$, Lemma 3.5 gives $T_1 \geq 1$ for $p \geq 9n^2$, and Lemma 3.6 gives $T_1 \geq 1$ for $n < p \leq 9n^2$.

Suppose next that $q \geq p^2$. By Lemma 6.1 with $k - n$ variables, the number of solutions of (6.1) is at least $q^{\,k-2n} - (nq^{1/2})^{\,k-n}$, which is positive if and only if $q^{\,k-3n} > n^{2(k-n)}$. Since

$q \ge p^2$ and $k > 3n$, it suffices to show $p^{k-3n} > n^{k-n}$, that is, $(p/n)^{k-3n} > n^{2n}$. We have $p \ge n+1$ and $\ln(1+1/n) > 1/(n+1)$, so

$$\left(\tfrac{p}{n}\right)^{k-3n} \;\ge\; \left(1+\tfrac{1}{n}\right)^{k-3n} \;>\; \exp\left(\frac{k-3n}{n+1}\right) \;\ge\; n^{2n},$$

where the last inequality holds because $k - 3n \ge 32n^2 \ln n - 1 - 2n \ge 2n(n+1)\ln n$ for $n \ge 3$. □

Theorem 6.5. *Let $n \ge 3$, let K be a number field, and let $\wp$ be a prime ideal of $\mathcal{O}_K$ above a rational prime $p > n$, with $q = N(\wp)$. Let $k_2 = \lfloor 32n^2 \ln n \rfloor + n$ be as in Lemma 3.7.*

(i) If $k \ge k_2$, then $W(\wp^h, k) \ge q^{\,n-k_2}\, q^{\,h(k-n)}$ for every $h \ge 1$, and $\sigma_\wp \ge q^{\,n-k_2}$.

(ii) If $q \ge 9n^2$ and $k \ge 6n^2$, then $W(\wp^h, k) \ge (1-q^{-3})\, q^{\,h(k-n)}$ for every $h \ge 1$, and $\sigma_\wp \ge 1 - q^{-3}$.

In both cases, the lower bound for $\sigma_\wp$ does not depend on $N_1, \ldots, N_n$.

Proof. (i) Let $k = k_2$. Lemma 6.4 gives $W_1 \ge 1$, and Lemma 6.3(ii) gives, for all $N_1, \ldots, N_n$,

$$W(\wp^h, k_2) \;\ge\; q^{\,(h-1)(k_2-n)} \;=\; q^{\,n-k_2}\, q^{\,h(k_2-n)}.$$

Lemma 5.12 extends the bound to all $k \ge k_2$.

(ii) By Lemma 6.1 with $F = \mathcal{O}_K/\wp$ and Lemma 6.2, $W(\wp, k) \ge q^{\,k-n}\big(1 - n^k q^{\,n-k/2}\big) \ge q^{\,k-n}(1-q^{-4})$. By Lemma 6.3(i) and Lemma 6.2,

$$W_1 \;\ge\; q^{\,k-n}(1-q^{-4}) - q^{\,k-n-4} \;=\; q^{\,k-n}(1-2q^{-4}) \;\ge\; q^{\,k-n}(1-q^{-3}),$$

and Lemma 6.3(ii) gives $W(\wp^h, k) \ge q^{\,(h-1)(k-n)}\, W_1 \ge (1-q^{-3})\, q^{\,h(k-n)}$.

In both cases, the constant does not depend on h, and $k \ge k_2 > n(n+1)$ in case (i) and $k \ge 6n^2 > n(n+1)$ in case (ii). Hence Lemma 4.25, applied with $h_\wp = 1$, gives the lower bounds for $\sigma_\wp$. □

The condition $q \ge 9n^2$ in (ii) holds if $f \ge 2$ and $p \ge 3n$, and for $f = 1$ it means $p \ge 9n^2$.

6.2 The Arithmetic Condition for a Field of Degree m

Recall from Section 5.2 the polynomials $t_r(X) = \binom{X}{r}\binom{n-X}{n-r}$, $0 \le r \le n$, for which (5.1) and (5.2) hold and $t_r(z) \in \mathbb{Z}$ for every integer z.

Lemma 6.6. *Let $n \ge 1$, let $\omega_1, \dots, \omega_m$ be an integral basis of the number field K of degree m, and let $t_r(X)$, $0 \le r \le n$, be the polynomials of Section 5.2. Let $x = a_1\omega_1 + \cdots + a_m\omega_m$ with $a_1, \dots, a_m \in \mathbb{Z}$. For $\boldsymbol{r} = (r_1, \dots, r_m)$ with $0 \le r_i \le n$, let*

$$t_{\boldsymbol{r}} = t_{r_1}(a_1) \cdots t_{r_m}(a_m), \qquad g_{\boldsymbol{r}} = r_1\omega_1 + \cdots + r_m\omega_m.$$

Then $t_{\boldsymbol{r}} \in \mathbb{Z}$,

$$\sum_{\boldsymbol{r}} t_{\boldsymbol{r}}\, g_{\boldsymbol{r}}^s = x^s, \qquad s = 1, \dots, n, \tag{6.2}$$

and $\sum_{\boldsymbol{r}} t_{\boldsymbol{r}} = 1$. Moreover, the term with $\boldsymbol{r} = (0, \dots, 0)$ in (6.2) is zero, so only the $(n+1)^m - 1$ non-zero points $g_{\boldsymbol{r}}$ occur. These points are non-zero since $\omega_1, \dots, \omega_m$ are linearly independent over $\mathbb{Q}$.

Proof. For $m = 2$, this is Lemma 5.2, and the proof is the same, with (5.1) applied once to each of the m coordinates. Fix $1 \le s \le n$. We show by induction on $j = 0, 1, \dots, m$ that

$$x^s = \sum_{r_1=0}^{n} \cdots \sum_{r_j=0}^{n} t_{r_1}(a_1) \cdots t_{r_j}(a_j)\big(r_1\omega_1 + \cdots + r_j\omega_j + a_{j+1}\omega_{j+1} + \cdots + a_m\omega_m\big)^s.$$

For $j = 0$, this is $x^s = (a_1\omega_1 + \cdots + a_m\omega_m)^s$. Suppose that the identity holds for some $j < m$, and fix $r_1, \dots, r_j$. The expression

$$\big(r_1\omega_1 + \cdots + r_j\omega_j + X\omega_{j+1} + a_{j+2}\omega_{j+2} + \cdots + a_m\omega_m\big)^s$$

is a polynomial in X of degree at most $s \le n$ with coefficients in K, so by (5.1) it equals

$$\sum_{r_{j+1}=0}^{n} t_{r_{j+1}}(X)\big(r_1\omega_1 + \cdots + r_{j+1}\omega_{j+1} + a_{j+2}\omega_{j+2} + \cdots + a_m\omega_m\big)^s.$$

Evaluating at $X = a_{j+1}$ and substituting the result into the induction hypothesis, we obtain the identity for $j+1$. The case $j = m$ is (6.2). By (5.2),

$$\sum_{\boldsymbol{r}} t_{\boldsymbol{r}} = \prod_{j=1}^{m} \Big(\sum_{r_j=0}^{n} t_{r_j}(a_j) \Big) = 1.$$

Each $t_{\boldsymbol{r}}$ is a product of integers, and the term with $\boldsymbol{r} = (0, \dots, 0)$ is $t_{\boldsymbol{0}} \cdot 0^s = 0$ for $s \ge 1$. □

Definition 5.3 of Condition (M) applies to every number field. Below, G denotes the set of the numbers $g_{\boldsymbol{r}}$ with $\boldsymbol{r} \neq (0, \ldots, 0)$. Distinct $\boldsymbol{r}$ give distinct numbers $g_{\boldsymbol{r}}$, since $\omega_1, \ldots, \omega_m$ are linearly independent over $\mathbb{Q}$, so G has $(n+1)^m - 1$ elements. For $m = 2$, this is the set G of Section 5.5.

Lemma 6.7. *Let $n \geq 1$, let K be a number field of degree m, and let G be as above.*

(i) $\Gamma_n(\mathcal{O}_K)$ is generated by the $(n+1)^m - 1$ vectors $(g, g^2, \ldots, g^n)$ with $g \in G$. Hence Condition (M) *of Definition 5.3 holds if and only if the system*

$$\sum_{g \in G} t_g \, g^s = N_s, \qquad s = 1, \ldots, n,$$

has a solution in integers t_g.

(ii) If the system $x_1^s + \cdots + x_k^s = N_s$, $s = 1, \ldots, n$, has a solution with $x_1, \ldots, x_k \in \mathcal{O}_K$, then Condition (M) *holds. So Condition* (M) *is necessary for the solubility of the system.*

Proof. The proof is that of Lemma 5.4, with Lemma 6.6 in place of Lemma 5.2. □

6.3 Unramified Prime Ideals of Residue Degree One

Throughout this section, $\wp$ is an unramified prime ideal of residue degree one above a rational prime $p \leq n$. That is, $e = f = 1$, so that $N(\wp) = p$ and $v_\wp(p) = 1$. Section 5.3 used only these two facts and the integral basis, so its results hold for $\wp$.

Theorem 6.8. *Let $n \geq 3$, let K be a number field of degree m, let $\wp$ be an unramified prime ideal of $\mathcal{O}_K$ of residue degree one above the rational prime p with $p \leq n$, and suppose that $N_1, \ldots, N_n$ satisfy Condition* (M) *of Definition 5.3. Then, for $k \geq k_1 = n^2 2^{2n-1}$ and every $h \geq 1$,*

$$W(\wp^h, k) \;\geq\; c_*^{\mathbb{Q}} \, N(\wp)^{h(k-n)}, \qquad c_*^{\mathbb{Q}} = p^{(2\varkappa + 2\delta + 1)(n - k_1)},$$

where $\varkappa$ and δ are as in Lemma 3.4. Hence $\sigma_\wp \geq c_*^{\mathbb{Q}} > 0$.

Proof. Let $h \geq 1$. The proof of Lemma 5.5(i) and (ii) uses only $v_\wp(p) = 1$ and $|\mathcal{O}_K/\wp^h| = N(\wp)^h = p^h$, so $\wp^h \cap \mathbb{Z} = p^h\mathbb{Z}$ and the reduction map $\phi_h \colon \mathbb{Z}/p^h\mathbb{Z} \to \mathcal{O}_K/\wp^h$ is a ring isomorphism. Hence there are integers $c_{1,h}, \ldots, c_{m,h}$, unique modulo p^h, with $\omega_i \equiv c_{i,h}$

(mod $\wp^h$) for $1 \le i \le m$. Write $N_s = a_{s,1}\omega_1 + \cdots + a_{s,m}\omega_m$ with $a_{s,i} \in \mathbb{Z}$, and let $\tilde{N}_s = a_{s,1}c_{1,h} + \cdots + a_{s,m}c_{m,h}$ for $s = 1, \ldots, n$, so that $N_s \equiv \tilde{N}_s \pmod{\wp^h}$. The proofs of Lemmas 5.6 and 5.7 use $\wp$ only through the isomorphism ϕ_h and the congruence $N_s \equiv \tilde{N}_s \pmod{\wp^h}$, so they apply to $\wp$ with $\tilde{N}_s$ in this form. They give $W(\wp^h, k) = W(p^h, k)$, where $W(p^h, k)$ is the counting function of Chapter 3 with $\tilde{N}_1, \ldots, \tilde{N}_n$ in place of $N_1, \ldots, N_n$, and, under Condition (M), natural numbers $\hat{N}_1, \ldots, \hat{N}_n$ that satisfy condition (3.1) and $\hat{N}_s \equiv \tilde{N}_s \pmod{p^h}$. The proof of Theorem 5.8 uses only these two facts, and it applies without change. □

6.4 Prime Ideals above $p \le n$

Throughout this section, $\wp$ is a prime ideal above a rational prime $p \le n$, of ramification index e and residue degree f, so that $v_\wp(p) = e$ and $N(\wp) = p^f$, and $\varpi \in \wp \setminus \wp^2$ and the complete residue system R modulo $\wp$ are as in Section 5.4, so that $v_\wp(z) = e\, v_p(z)$ for every non-zero integer z by (5.5). If $e \ge 2$ or $f \ge 2$, the reduction $\mathbb{Z} \to \mathcal{O}_K/\wp^h$ is not surjective for $h \ge 2$, so there is no isomorphism like ϕ_h, and we work in $\mathcal{O}_K$ as in Section 5.5. Recall from Lemma 3.4 that $p^\varkappa \le n < p^{\varkappa+1}$ and $\delta = v_p\big((n-1)!\big)$, from (5.7) that $\alpha = 2(\varkappa+\delta)e+1$ and $\beta = (\varkappa+\delta)e+1$, and that $\alpha_0 = 2\varkappa + 2\delta + 1$. Recall also that G is the set of the $(n+1)^m - 1$ non-zero points $g_{\boldsymbol{r}}$ of Section 6.2.

Proposition 6.9. *Let $n \ge 3$, let K be a number field of degree m, let $\wp$ be a prime ideal of $\mathcal{O}_K$ above the rational prime $p \le n$, and let $N_1, \ldots, N_n \in \mathcal{O}_K$. Then Lemmas 5.13, 5.14 and 5.15 hold for $\wp$. If, moreover, $N_1, \ldots, N_n$ satisfy Condition* (M) *of Definition 5.3, then, with*

$$k_0 \;=\; n + \big((n+1)^m - 1\big)\big(p^{\alpha_0} - 1\big),$$

we have $W(\wp^h, k) \ge N(\wp)^{\alpha(n-k_0)}\, N(\wp)^{h(k-n)}$ for every $k \ge k_0$ and every $h \ge 1$.

Proof. The proofs of Lemmas 5.13, 5.14 and 5.15 use, besides the lemmas of Section 5.4, only the uniformizer ϖ, the identity (5.5), the residue system R and the conditions (5.6), which hold for every $e \ge 1$. Hence they apply to $\wp$ without change. The proof of Proposition 5.16 uses, besides these lemmas, only the property of G in Lemma 5.4(i), which for the set G of Section 6.2 is Lemma 6.7(i), and the inequality $v_\wp(p^{\alpha_0}) = e\alpha_0 \ge \alpha$. Hence it applies to $\wp$ with $(n+1)^m - 1$ in place of $(n+1)^2 - 1$. □

Theorem 6.10. *Let $n \ge 3$, let K be a number field of degree m, and let $\wp$ be a prime ideal of $\mathcal{O}_K$ above the rational prime p with $p \le n$, and suppose that $N_1, \ldots, N_n$ satisfy*

Condition (M) *of Definition 5.3. Let*

$$k_3 = (n+1)^m\, n^2 2^{2n-1}.$$

Then, for $k \geq k_3$ and every $h \geq 1$,

$$W(\wp^h, k) \;\geq\; c_*^{\mathrm{gen}}\, N(\wp)^{h(k-n)}, \qquad c_*^{\mathrm{gen}} = \big(n^2 2^{2n-1}\big)^{\,m(n-k_3)}.$$

Hence $\sigma_\wp \geq c_*^{\mathrm{gen}} > 0$.

Proof. Let k_0 be as in Proposition 6.9. By Lemma 5.11, $p^{\alpha_0} \leq n^2 2^{2n-1}$, so

$$k_0 \;\leq\; n + \big((n+1)^m - 1\big)\, n^2 2^{2n-1} \;\leq\; (n+1)^m\, n^2 2^{2n-1} \;=\; k_3,$$

using $n \leq n^2 2^{2n-1}$, and, since $\alpha \leq e\alpha_0$ and $ef \leq m$,

$$N(\wp)^\alpha = p^{f\alpha} \;\leq\; p^{fe\alpha_0} \;\leq\; \big(p^{\alpha_0}\big)^m \;\leq\; \big(n^2 2^{2n-1}\big)^m.$$

For $k \geq k_3$, we therefore have

$$N(\wp)^{\alpha(n-k_0)} \;\geq\; N(\wp)^{\alpha(n-k_3)} \;\geq\; \big(n^2 2^{2n-1}\big)^{m(n-k_3)} \;=\; c_*^{\mathrm{gen}},$$

and Proposition 6.9 gives $W(\wp^h, k) \geq c_*^{\mathrm{gen}}\, N(\wp)^{h(k-n)}$. The constant does not depend on h, and $k \geq k_3 > n(n+1)$, so Lemma 4.25, applied with $h_\wp = 1$, gives $\sigma_\wp \geq c_*^{\mathrm{gen}}$. □

6.5 Lower Bound for the Singular Series

Recall that $\sigma = \prod_\wp \sigma_\wp$ for $k > n(n+1)$ (Lemma 4.22), and that $\pi(n)$ denotes the number of primes $p \leq n$. The following is the main theorem of this thesis.

Theorem 6.11. *Let $n \geq 3$, and let K be a number field of degree m. Suppose that $N_1, \ldots, N_n$ satisfy Condition* (M) *of Definition 5.3 and that*

$$k \;\geq\; k_3 \;=\; (n+1)^m\, n^2 2^{2n-1}.$$

Then

$$\sigma \;\geq\; \exp\big(-2m\zeta(3)\big)\, \big(c_*^{\mathrm{gen}}\big)^{m\pi(n)} \Big(\prod_{n<p<9n^2} p\Big)^{-mk_2} \;>\; 0,$$

where $\pi(n)$ is the number of primes $p \leq n$, $\zeta(3) = \sum_{j\geq 1} j^{-3}$, c_*^{gen} is the constant of Theorem 6.10, and $k_2 = \lfloor 32n^2 \ln n \rfloor + n$.

Proof. Since $k \geq k_3 > n(n+1)$, Lemma 4.22 gives $\sigma = \prod_{\wp} \sigma_{\wp}$, the product being absolutely convergent, and we divide the prime ideals into three classes. Every rational prime p has at most m prime ideals above it, each of norm at least p, and $\sum_{\wp|p} f_{\wp} \leq m$.

Let $p \leq n$. There are at most $m\pi(n)$ such $\wp$, and Theorem 6.10 gives $\sigma_{\wp} \geq c_*^{\mathrm{gen}}$.

Let $p > n$ and $N(\wp) < 9n^2$, so that $p < 9n^2$. We have $k_2 = \lfloor 32n^2 \ln n \rfloor + n \leq 33n^3 \leq k_3$, where the last inequality reduces to $33n \leq (n+1)^m 2^{2n-1}$, which holds for $n \geq 3$ and $m \geq 1$. Hence Theorem 6.5(i) gives $\sigma_{\wp} \geq N(\wp)^{n-k_2} \geq N(\wp)^{-k_2}$. For a fixed p, the product of $\sigma_{\wp}$ over the prime ideals $\wp$ above p with $N(\wp) < 9n^2$ is at least $p^{-k_2 \sum_{\wp|p} f_{\wp}} \geq p^{-mk_2}$, so the product over all these $\wp$ is at least $\big(\prod_{n<p<9n^2} p\big)^{-mk_2}$.

Let $p > n$ and $N(\wp) \geq 9n^2$. Since $k \geq k_3 \geq 6n^2$, Theorem 6.5(ii) gives $\sigma_{\wp} \geq 1 - N(\wp)^{-3}$. We have $1 - x \geq \exp(-2x)$ for $0 \leq x \leq \frac{1}{2}$, since $\ln(1-x) + 2x$ vanishes at $x = 0$ and has derivative $2 - (1-x)^{-1} \geq 0$ on this interval. Hence

$$\prod_{\substack{p>n \\ N(\wp)\geq 9n^2}} \sigma_{\wp} \;\geq\; \exp\Big(-2\sum_{\wp} N(\wp)^{-3}\Big) \;\geq\; \exp\Big(-2m\sum_{p} p^{-3}\Big) \;\geq\; \exp\big(-2m\zeta(3)\big).$$

Multiplying the three bounds gives the theorem. □

6.6 Future Work

Theorem 6.11 bounds σ below by a positive constant independent of $N_1, \ldots, N_n$ for $k \geq k_3 = (n+1)^m n^2 2^{2n-1}$. Over $\mathbb{Z}$, the least number of variables is $k_{\min}(n) = H(n)$ for $n \geq 12$, which has order 2^n (Chapter 1), while the bound $k_1 = n^2 2^{2n-1}$ of Lemma 3.4, which Chapter 5 follows, has order $n^2 2^{2n}$, and $k_3 = (n+1)^m k_1$. We would like to pursue the following questions further.

(i) The least number of variables. Over $\mathbb{Z}$, Mit'kin [17, 18] proved that $k_{\min}(n) = H(n)$ for $n \geq 12$. For $3 \leq n \leq 11$, the value of $k_{\min}(n)$ is not known, and whether his argument extends to $\mathcal{O}_K$ is open. The least k for which σ is bounded below by a positive constant independent of $N_1, \ldots, N_n$ under Condition (M), and how it grows with n and m, is not known.

(ii) The number of points in Condition (M). Lemma 6.7 gives $(n+1)^m - 1$ generators of $\Gamma_n(\mathcal{O}_K)$ of the form $(x, x^2, \ldots, x^n)$, and this number enters k_3 as the factor $(n+1)^m$, through the number of variables in Proposition 6.9. As a subgroup of $\mathcal{O}_K^n \cong \mathbb{Z}^{mn}$,

$\Gamma_n(\mathcal{O}_K)$ is generated by at most mn vectors, but these might not be of the form $(x, x^2, \dots, x^n)$, which the construction of Proposition 6.9 needs. Whether the factor $(n+1)^m$ in k_3 can be replaced by a power of mn is not known to the author.

(iii) The dependence on p. The bound k_3 and the constant c_*^{gen} are uniform in the prime ideal $\wp$, and for a fixed prime $p \leq n$ the number $k_0 = n + \big((n+1)^m - 1\big)\big(p^{\alpha_0} - 1\big)$ of variables in Proposition 6.9 is smaller than k_3. The best bound for every prime ideal is not determined.

(iv) Systems with coefficients. This thesis considers the system $x_1^s + \dots + x_k^s = N_s$. For fixed non-zero coefficients $a_1, \dots, a_k \in \mathcal{O}_K$ and the system

$$a_1 x_1^s + \dots + a_k x_k^s = N_s, \qquad s = 1, \dots, n,$$

the Gauss sums and the singular series are defined in the same way, but Condition (M) and the construction of the local solutions in Chapters 5 and 6 use that all coefficients are 1. We do not treat the case of general coefficients in this thesis.

References

[1] G. I. Arkhipov. On the value of the singular series in the Hilbert–Kamke problem. *Doklady Akademii Nauk SSSR*, 259(2):265–267, 1981. English translation: Soviet Mathematics Doklady 24 (1981), no. 1, 49–51.

[2] G. I. Arkhipov. On the Hilbert–Kamke problem. *Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya*, 48(1):3–52, 1984. English translation: Mathematics of the USSR-Izvestiya 24 (1985), no. 1, 1–47.

[3] G. I. Arkhipov, V. N. Chubarikov, and A. A. Karatsuba. *Trigonometric Sums in Number Theory and Analysis*, volume 39 of *De Gruyter Expositions in Mathematics*. Walter de Gruyter, Berlin, 2004.

[4] J. Brüdern and T. D. Wooley. On Waring's problem for larger powers. *Journal für die reine und angewandte Mathematik*, 805:115–142, 2023.

[5] M. J. Greenberg. Rational points in Henselian discrete valuation rings. *Publications Mathématiques de l'IHÉS*, 31:59–64, 1966.

[6] G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio Numerorum'; I: A new solution of Waring's problem. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, pages 33–54, 1920.

[7] G. H. Hardy and S. Ramanujan. Asymptotic formulae in combinatory analysis. *Proceedings of the London Mathematical Society (2)*, 17:75–115, 1918.

[8] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman.

[9] D. Hilbert. Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem). *Mathematische Annalen*, 67(3):281–300, 1909.

[10] L.-K. Hua. On Waring's problem. *The Quarterly Journal of Mathematics (Oxford Series)*, 9:199–202, 1938.

[11] L.-K. Hua. On exponential sums over an algebraic number field. *Canadian Journal of Mathematics*, 3:44–51, 1951.

[12] E. Kamke. Verallgemeinerungen des Waring-Hilbertschen Satzes. *Mathematische Annalen*, 83:85–112, 1921.

[13] S. Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[14] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[15] D. A. Marcus. *Number Fields*. Universitext. Springer, Cham, second edition, 2018.

[16] K. K. Mardzhanishvili. Sur la représentation simultanée de n nombres par des sommes des puissances complètes [On the simultaneous representation of n numbers by sums of complete powers]. *Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya*, 1(4):609–631, 1937. In French; the author's name is printed there as C. Mardjanichvili.

[17] D. A. Mit'kin. An estimate for the number of terms in the Hilbert–Kamke problem. *Matematicheskii Sbornik (N.S.)*, 129(171):549–577, 1986. No. 4. English translation: Mathematics of the USSR-Sbornik 57 (1987), no. 2, 561–590.

[18] D. A. Mit'kin. An estimate for the number of terms in the Hilbert–Kamke problem. II. *Matematicheskii Sbornik (N.S.)*, 132(174):345–351, 1987. No. 3. English translation: Mathematics of the USSR-Sbornik 60 (1988), no. 2, 339–346.

[19] C. L. Siegel. Generalization of Waring's problem to algebraic number fields. *American Journal of Mathematics*, 66(1):122–136, 1944.

[20] C. L. Siegel. Sums of m-th powers of algebraic integers. *Annals of Mathematics (2)*, 46:313–339, 1945.

[21] R. C. Vaughan. *The Hardy–Littlewood Method*, volume 125 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, second edition, 1997.

[22] R. C. Vaughan and T. D. Wooley. Waring's problem: a survey. In *Number Theory for the Millennium, III (Urbana, IL, 2000)*, pages 301–340. A K Peters, Natick, MA, 2002.

[23] I. M. Vinogradov. A new solution of Waring's problem. *Doklady Akademii Nauk SSSR*, 2:337–341, 1934. No. 6. In Russian.

[24] I. M. Vinogradov. *The Method of Trigonometrical Sums in the Theory of Numbers*. Interscience Publishers, London and New York, 1954. Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport.

[25] Y. Wang. *Diophantine Equations and Inequalities in Algebraic Number Fields*. Springer-Verlag, Berlin, 1991.

[26] E. Waring. *Meditationes Algebraicae*. J. Archdeacon, Cambridge, 1770.

[27] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Mathematische Annalen*, 77:313–352, 1916.

[28] A. Wieferich. Beweis des Satzes, daß sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen läßt. *Mathematische Annalen*, 66:95–101, 1909.

[29] T. D. Wooley. Nested efficient congruencing and relatives of Vinogradov's mean value theorem. *Proceedings of the London Mathematical Society (3)*, 118:942–1016, 2019. No. 4.

[30] T. D. Wooley. Subconvexity and the Hilbert–Kamke problem. *Mathematische Zeitschrift*, 311, 2025. Paper No. 17, 14 pp.