

## Almost universality of a sum of norms

Jeongho PARK

(Received March 24, 2014)

(Revised June 23, 2015)

**ABSTRACT.** In this paper the author considers a particular type of polynomials with integer coefficients, consisting of a perfect power and two norm forms of abelian number fields with coprime discriminants. It is shown that such a polynomial represents every natural number with only finitely many exceptions. The circle method is used, and the local class field theory played a central role in estimating the singular series.

### 1. Introduction

Let  $f = f(\vec{\zeta}) = f(\zeta_1, \zeta_2, \dots)$  be an integer-valued polynomial in many variables that is *locally universal*, meaning that for any  $n \in \mathbf{N}$  and a prime  $p$

$$f(\vec{\zeta}) = n \tag{1.1}$$

is soluble with  $\zeta_i \in \mathbf{Z}_p$ . When (1.1) is soluble for all  $n \in \mathbf{N}$  in integers  $\zeta_1, \zeta_2, \dots$ ,  $f$  is said to be *universal*, and when it is soluble for all but finitely many  $n \in \mathbf{N}$  it is *almost universal*. It is quite often the case that  $f$  is not universal or even almost universal as indicated by the Brauer-Manin obstruction. The failure of the Hasse principle, though, can be in some sense overcome if we allow more variables in the equation. It is a general phenomenon that if a surface  $\mathcal{S}(n)$  of a higher dimension, defined by  $F(\vec{z}) = n$ , contains the original surface  $\mathcal{S}_0(n)$  given by  $f(\vec{\zeta}) = n$  as a section, then it becomes almost universal, provided their codimension is sufficiently large. The Hardy-Littlewood method provides a powerful tool for estimating the number of variables necessary for this.

Although this analytic method is powerful for many problems of additive nature, it has some technical limitations and a factor of  $\log(\deg f)$  is invincible in general; most of the results satisfy  $\dim(\mathcal{S}(n))/\dim(\mathcal{S}_0(n)) \gg \log(\deg f)$ . The term  $\log(\deg f)$  arises from the technical difficulty to handle the minor arcs. If one considers a specific polynomial that is irrelevant of this difficulty, it is provable that  $\log(\deg f)$  reduces to  $O(1)$ .

---

Supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (2010-0026473).

2010 *Mathematics Subject Classification*. Primary 11P05, 11D85; Secondary 11P55, 11D57.

*Key words and phrases*. Waring's problem, Hardy Littlewood method, universal form, norm form.

In the 1960s, Birch, Davenport and Lewis already observed this and considered a specific type of  $k$ -forms. Let  $K, E$  be the number fields of degree  $k$  with integral bases  $\{\omega_1, \dots, \omega_k\}, \{\omega'_1, \dots, \omega'_k\}$ . Denote the norm of  $x_1\omega_1 + \dots + x_k\omega_k$  and  $y_1\omega'_1 + \dots + y_k\omega'_k$  by  $N_K(x_1, \dots, x_k)$  and  $N_E(y_1, \dots, y_k)$ . In [1] they considered  $z^k + N_K(x_1, \dots, x_k) + N_E(y_1, \dots, y_k)$  under some provisos, reached the following theorem as their main result.

**THEOREM 1.1.** *Suppose  $K, E$  are not both totally complex, and let  $\delta_K, \delta_E$  denote their discriminants. Suppose that, for every prime  $p$  dividing both  $\delta_K$  and  $\delta_E$ , the equation*

$$n = z^k + N_K(x_1, \dots, x_k) + N_E(y_1, \dots, y_k) \quad (1.2)$$

*has a non-singular solution in the  $p$ -adic field. Then (1.2) has infinitely many solutions in integers.*

The strategy in their work was to follow the routine procedure of the circle method, except for the treatment of the singular series. A typical way of dealing with the singular series is to obtain an estimate of exponential sums  $S_{a,q} = \sum_{\vec{\xi} \bmod q} e(af(\vec{\xi})/q)$  by factoring them into products of exponential sums over a single variable. But a norm form  $N_K(x_1, \dots, x_k)$  has many off-diagonal terms and it is not easy to do that directly. In [1] instead, a technique invented by Birch was used to get an auxiliary lemma of the type  $\sum_{q \leq X} q^{-2k} \sum_{\substack{a=1 \\ (a,q)=1}}^q |S_{a,q}|^2 \ll X^\epsilon$ . They also showed the positivity of the singular series, but without giving an estimate of its range.

In this study we prove the almost universality of the polynomial  $z^{k_0} + N_K(\vec{x}) + N_E(\vec{y})$  in a different setting that enlightens several new aspects. We treat abelian number fields  $K, E$  whose degrees  $k_1, k_2$  may be different and can be totally imaginary as well. We also provide an effective bound for the singular series. In the last section we will include an example which shows the optimality of our conclusion, i.e., that the sum of two norms can fail to be almost universal even when it is locally universal. There are very few optimal results in the theory of additive problems, but this result seems to provide one of them.

The techniques in [1] may help us deduce some parts of our results, but will not exhaust the contents of this research. On a technical point of view, the significance of this study is that estimates of the exponential sum  $S_{a,q}$  uses local class field theory and a restricted sum, which plays an essential role in dealing with the singular series by removing solutions that are  $p$ -adically singular for a ‘bad’ prime  $p$ . (Here ‘bad’ means that either  $p$  is too small or it is ramified in one of  $K, E$ .)

This article is organized as follows. In Section 2 we give some definitions, in particular of the congruence residue classes  $\check{R}_Q$  and  $\check{\mathfrak{B}}(n)$  that will be

important in the treatment of the major arcs. In Section 3 we reduce the integration over major arcs into singular series and singular integral. The estimation of the singular series follows in three subsequent sections. Section 4 covers the exponential sums over bad primes. Section 5 gives some basics about algebraic number theory, which will be used in Section 6 to design a particular system of representatives of  $O_K/p^L O_K$ , together with local class field theory, in order to obtain a successful bound of  $S_{a,p^L}$  for good primes  $p$ . Section 7 lays down a fairly classical argument on the singular integral. We omit estimation on the minor arcs because the reasoning in [1] carries over verbatim. The last section gives the desired asymptotic formula and describes how to construct a sum of two norms that is locally universal but is not almost universal, demonstrating why the term  $z^k$  is necessary in our problem.

## 2. Notations and settings

Let  $K$  and  $E$  be abelian number fields with ring of integers  $O_K$ ,  $O_E$  and integral bases  $\{\varphi_1, \dots, \varphi_{k_1}\}$  and  $\{\psi_1, \dots, \psi_{k_2}\}$  whose discriminants  $\delta_K$ ,  $\delta_E$  are relatively prime. Since  $(\delta_K, \delta_E) = 1$ , for each rational prime  $p$  at least one of the inertial groups  $\mathfrak{I}_K(p)$ ,  $\mathfrak{I}_E(p)$  is trivial. Suppose  $\mathfrak{I}_K(p)$  is trivial. Let  $\mathfrak{p}_1, \dots, \mathfrak{p}_g$  be the prime ideals in  $K$  above  $p$ , and  $O_{K,\mathfrak{p}_i}$  the completion of  $O_K$  at  $\mathfrak{p}_i$ . The local class field theory says that the local norm map  $N_{K,i} : (O_{K,\mathfrak{p}_i})^* \rightarrow (\mathbf{Z}_p)^*$  is surjective. We also know that  $N_K(\alpha) = \prod_{i=1}^g N_{K,i}(\alpha)$  for  $\alpha \in K$ , where we consider  $\alpha$ ,  $N_K(\alpha)$  as elements in adequate completions of  $K$  [6]. Since  $O_K$  embeds into  $\prod_{i=1}^g O_{K,\mathfrak{p}_i}$  as a dense subset, combining the surjectivity of  $N_{K,i}$ , the local universality of  $N_K(\vec{x}) + N_E(\vec{y}) = N_{K|\mathbf{Q}}(\vec{x} \cdot \vec{\varphi}) + N_{E|\mathbf{Q}}(\vec{y} \cdot \vec{\psi})$  will follow if the local norm maps  $N_{K,1}, \dots, N_{K,g}$  are all continuous. But  $N_{K,i}$  is indeed continuous as we easily see. Choose a uniformizer  $\pi \in \mathfrak{p}_i$  in  $O_{K,\mathfrak{p}_i}$ . Any element  $\sigma \in \text{Gal}(K_{\mathfrak{p}_i}|\mathbf{Q}_p)$  maps  $\pi$  to another uniformizer in  $O_{K,\mathfrak{p}_i}$ , so for an element  $y \in O_{K,\mathfrak{p}_i}$  we can write  $(y\pi^\ell)^\sigma = \tilde{y}(\sigma)\pi^\ell$  for some  $\tilde{y}(\sigma) \in O_{K,\mathfrak{p}_i}$ . Thus for  $x, y \in O_{K,\mathfrak{p}_i}$ , one has

$$N_{K,i}(x + y\pi^\ell) = \prod_{\sigma} (x + y\pi^\ell)^\sigma = \prod_{\sigma} (x^\sigma + \tilde{y}(\sigma)\pi^\ell) = N_{K,i}(x) + \pi^\ell z$$

for some  $z \in O_{K,\mathfrak{p}_i}$ . But  $\pi^\ell z = N_{K,i}(x + y\pi^\ell) - N_{K,i}(x) \in \mathfrak{p}_i^\ell \cap \mathbf{Z}_p$ , whence we have  $N_{K,i}(x + y\pi^\ell) \equiv N_{K,i}(x) \pmod{p^\ell}$ . It follows that  $N_{K,i}$  is a continuous map, and the sum of norms  $N_K(\vec{x}) + N_E(\vec{y})$  is therefore locally universal.

Throughout this paper we write

$$\begin{aligned} F(\vec{z}) &= F(z_0, z_1, \dots, z_{k_1+k_2}) = F(z_0, x_1, \dots, x_{k_1}, y_1, \dots, y_{k_2}) \\ &= F(z_0, \vec{x}, \vec{y}) = z_0^{k_0} + N_K(\vec{x}) + N_E(\vec{y}). \end{aligned}$$

$e(\alpha)$  denotes  $e^{2\pi i\alpha}$  and  $v_p$  denotes the  $p$ -adic valuation as in tradition.  $\mathbf{P}$  denotes the set of rational primes. We put  $Q = \prod_{p \in \check{\mathbf{P}}} p$  where

$$\check{\mathbf{P}} = \{p \in \mathbf{P} : p < (k_1 k_2)^{2k_0} \text{ or } p \mid \delta_K \delta_E\}.$$

In particular  $1 \ll Q \ll 1$  for fixed  $k_0, K$  and  $E$ .

Let  $\check{\mathbf{R}}_q^K$  be a system of representatives  $\vec{x}$  modulo  $q$  such that for any prime  $p$  in  $\check{\mathbf{P}}$  that divides  $q$ , one has  $N_K(\vec{x}) \not\equiv 0 \pmod{p}$ .  $\check{\mathbf{R}}_q^E$  is defined in the same manner, and let  $\check{\mathbf{R}}_q$  be a system of representatives  $\vec{z} = (z_0, \vec{x}, \vec{y}) \pmod{q}$  with  $\vec{x} \in \check{\mathbf{R}}_q^K$ ,  $\vec{y} \in \check{\mathbf{R}}_q^E$ . Note that  $|\check{\mathbf{R}}_{qr}| = |\check{\mathbf{R}}_q| |\check{\mathbf{R}}_r|$  if  $(q, r) = 1$ . For brevity in the sequel we write  $\vec{z} \equiv \check{\mathbf{R}}_q$  for an integral vector  $\vec{z}$  if  $\vec{z} \equiv \vec{a} \pmod{q}$  for some  $\vec{a} \in \check{\mathbf{R}}_q$ . Observe that  $\vec{z} \equiv \check{\mathbf{R}}_q$  for all  $q \geq 1$  if and only if  $\vec{z} \equiv \check{\mathbf{R}}_Q$ .

Throughout this article we let  $k = \max\{k_0, k_1, k_2\}$  and  $X_i = n^{1/k_i}$ . In the definition of major and minor arcs, we consider the Farey dissection of order  $n^{1-\nu}$  where  $\nu$  is a fixed small positive number, in particular, less than  $\frac{1}{5k}$ . For a technical reason in the estimation of the singular integral, we need to choose small boxes  $\mathfrak{B}_i$  in  $[0, 1]$ ,  $[0, 1]^{k_1}$  and  $[0, 1]^{k_2}$  so that  $\mathfrak{B} = \mathfrak{B}_0 \times \mathfrak{B}_1 \times \mathfrak{B}_2$  is around a nonsingular point of the Euclidean surface defined by  $F(\vec{\phi}) = 1$ . Let  $X_i \mathfrak{B}_i = \{\vec{r} : \frac{1}{X_i} \vec{r} \in \mathfrak{B}_i\}$ . The *restricted sum*  $\sum_{\vec{z} \in \check{\mathfrak{B}}(n)} e(\alpha F(\vec{z}))$  is defined over

$$\check{\mathfrak{B}}(n) = \{\vec{r} \in (X_0 \mathfrak{B}_0 \times X_1 \mathfrak{B}_1 \times X_2 \mathfrak{B}_2) \cap \mathbf{Z}^{1+k_1+k_2} : \vec{r} \equiv \check{\mathbf{R}}_Q\}.$$

$\check{\mathfrak{B}}^K(n)$  is defined similarly using  $X_1 \mathfrak{B}_1 \cap \mathbf{Z}^{k_1}$  and  $\check{\mathbf{R}}_Q^K$ , and so is  $\check{\mathfrak{B}}^E(n)$ . We want to estimate the number of solutions to  $F(\vec{z}) = n$  with  $\vec{z} \in \check{\mathfrak{B}}(n)$ , viz,

$$\check{r}(n) = \int_c^{1+c} \sum_{\vec{z} \in \check{\mathfrak{B}}(n)} e(\alpha F(\vec{z})) e(-n\alpha) d\alpha$$

for some real number  $c$ .

For simplicity we write  $\sum_{a \bmod^* q}$  to denote the summation over  $a$  that runs through 1 to  $q$  under the condition  $(a, q) = 1$ . We define the major arcs for  $1 \leq a \leq q \leq n^\nu$  and  $(a, q) = 1$  by

$$\mathfrak{M}(q, a) = \{\alpha : |\alpha - a/q| \leq n^{-1+\nu}\}, \quad \mathfrak{M} = \bigcup_{q \leq n^\nu} \bigcup_{a \bmod^* q} \mathfrak{M}(q, a)$$

and put the minor arcs  $\mathfrak{m} = (n^{\nu-1}, 1 + n^{\nu-1}] - \mathfrak{M}$ . Note that  $\mathfrak{M}$  is a disjoint union of the segments  $\mathfrak{M}(q, a)$ .

### 3. The major arcs

For each rational prime  $p$  and  $(a, p) = 1$ , let

$$S_{a, p^L}^K = \sum_{\vec{x} \bmod p^L} e\left(\frac{a}{p^L} N_K(\vec{x})\right), \quad \check{S}_{a, p^L}^K = \sum_{\vec{x} \in \check{\mathbf{R}}_{p^L}^K} e\left(\frac{a}{p^L} N_K(\vec{x})\right).$$

$S_{a,p^L}^E$  and  $\check{S}_{a,p^L}^E$  are defined in the same manner. For  $(a, q) = 1$  we also put

$$\check{S}_{a,q} = \sum_{\vec{z} \in \check{R}_q} e\left(\frac{a}{q}F(\vec{z})\right), \quad I(\beta) = \int_{X_0\mathfrak{B}_0 \times X_1\mathfrak{B}_1 \times X_2\mathfrak{B}_2} e(\beta F(\vec{r}))d\vec{r}.$$

Let  $\kappa(q)$  be the product of distinct prime factors of  $(q, Q)$ .

LEMMA 3.1. Assume  $|\beta| \leq n^{v-1}$ ,  $1 \leq a \leq q \leq n^v$ ,  $(a, q) = 1$ . Then

$$\begin{aligned} & \sum_{\vec{z} \in \check{\mathfrak{B}}(n)} e\left(\left(\frac{a}{q} + \beta\right)F(\vec{z})\right) \\ &= \frac{|\check{R}_Q|}{Q^{1+k_1+k_2}} \frac{\kappa(q)^{1+k_1+k_2}}{|\check{R}_{\kappa(q)}|} \frac{1}{q^{1+k_1+k_2}} \check{S}_{a,q} I(\beta) + O(n^{2+1/k_0-1/k+2v}) \end{aligned}$$

PROOF. Let  $q = \text{lcm}(q, Q) = q \frac{Q}{\kappa(q)}$  and write  $\vec{z} = q\vec{a} + \vec{b}$ ,  $0 \leq b_i < q$ . Let  $A(q, \vec{b}) = \{\vec{\eta} \in \mathbf{R}^{1+k_1+k_2} : q\vec{\eta} + \vec{b} \in X_0\mathfrak{B}_0 \times X_1\mathfrak{B}_1 \times X_2\mathfrak{B}_2\}$  and  $A(q, \vec{b}) = A(q, \vec{b}) \cap \mathbf{Z}^{1+k_1+k_2}$ . One easily has

$$\begin{aligned} \sum_{\vec{z} \in \check{\mathfrak{B}}(n)} e\left(\left(\frac{a}{q} + \beta\right)F(\vec{z})\right) &= \sum_{\vec{b} \in \check{R}_q} \sum_{\vec{a} \in A(q, \vec{b})} e\left(\frac{a}{q}F(q\vec{a} + \vec{b})\right) e(\beta F(q\vec{a} + \vec{b})) \\ &= \sum_{\vec{b} \in \check{R}_q} e\left(\frac{a}{q}F(\vec{b})\right) \sum_{\vec{a} \in A(q, \vec{b})} e(\beta F(q\vec{a} + \vec{b})). \end{aligned}$$

Let  $h : \mathbf{R}^{1+k_1+k_2} \rightarrow \mathbf{C}$  be a map defined by  $h(\vec{\eta}) = e(\beta F(q\vec{\eta} + \vec{b}))$ . If  $\vec{a}$  is an integral vector near  $\vec{\eta}$  so that  $|\eta_i - a_i| \leq 1/2$  for all  $0 \leq i \leq k_1 + k_2$ , and  $M$  is the supremum of the absolute value of directional derivatives of  $h(\vec{\eta})$  for  $\vec{\eta} \in A(q, \vec{b})$ , then clearly  $|h(\vec{\eta}) - h(\vec{a})| \ll M$ . Observe that any convex body  $U \subset A(q, \vec{b})$  can be divided into unit boxes together with at most  $O\left(\frac{X_0}{q}\left(\frac{X_1}{q}\right)^{k_1}\left(\frac{X_2}{q}\right)^{k_2}\left(\frac{q}{X_0} + \frac{q}{X_1} + \frac{q}{X_2}\right)\right)$  possible broken boxes. Hence

$$\begin{aligned} & \left| \int_{A(q, \vec{b})} h(\vec{\eta}) d\vec{\eta} - \sum_{\vec{a} \in A(q, \vec{b})} h(\vec{a}) \right| \\ & \ll \overline{|A(q, \vec{b})|} M + \frac{X_0 X_1^{k_1} X_2^{k_2}}{q^{k_1+k_2}} \left( \frac{1}{X_0} + \frac{1}{X_1} + \frac{1}{X_2} \right) \sup_{\vec{\eta}} |h(\vec{\eta})| \end{aligned}$$

where  $\overline{|A(q, \vec{b})|}$  is the Lebesgue measure of  $\overline{A(q, \vec{b})}$ . Here

$$\overline{|A(q, \vec{b})|} \ll \frac{X_0 X_1^{k_1} X_2^{k_2}}{q^{1+k_1+k_2}}, \quad \sup_{\vec{\eta}} |h(\vec{\eta})| = 1,$$

and

$$M \ll \sum_{i=0}^{k_1+k_2} \left| \frac{\partial}{\partial \eta_i} h(\vec{\eta}) \right| \ll \mathfrak{q} |\beta| (X_0^{k_0-1} + X_1^{k_1-1} + X_2^{k_2-1}) \ll \mathfrak{q} |\beta| n^{1-1/k}$$

which gives

$$\begin{aligned} \left| \int_{A(\mathfrak{q}, \vec{b})} h(\vec{\eta}) d\vec{\eta} - \sum_{\vec{a} \in A(\mathfrak{q}, \vec{b})} h(\vec{a}) \right| &\ll \frac{n^{2+1/k_0}}{\mathfrak{q}^{k_1+k_2}} n^{1-1/k} |\beta| + \frac{n^{2+1/k_0-1/k}}{\mathfrak{q}^{k_1+k_2}} \\ &\ll \frac{n^{2+1/k_0-1/k+v}}{\mathfrak{q}^{k_1+k_2}}. \end{aligned}$$

Writing  $\mathfrak{q}\vec{\eta} + \vec{b} = \vec{r}$ ,

$$\begin{aligned} \int_{A(\mathfrak{q}, \vec{b})} h(\vec{\eta}) d\vec{\eta} &= \int_{A(\mathfrak{q}, \vec{b})} e(\beta F(\mathfrak{q}\vec{\eta} + \vec{b})) d\vec{\eta} \\ &= \int_{X_0 \mathfrak{B}_0 \times X_1 \mathfrak{B}_1 \times X_2 \mathfrak{B}_2} e(\beta F(\vec{r})) d\vec{r} \frac{1}{\mathfrak{q}^{1+k_1+k_2}} \\ &= \frac{1}{\mathfrak{q}^{1+k_1+k_2}} I(\beta). \end{aligned}$$

Since  $\mathfrak{q} = q \frac{Q}{\kappa(q)}$ , one has

$$\sum_{\vec{b} \in \check{\mathbf{R}}_{\mathfrak{q}}} e\left(\frac{a}{q} F(\vec{b})\right) = |\check{\mathbf{R}}_{Q/\kappa(q)}| \sum_{\vec{b} \in \check{\mathbf{R}}_q} e\left(\frac{a}{q} F(\vec{b})\right) = |\check{\mathbf{R}}_{Q/\kappa(q)}| \check{S}_{a,q}.$$

It follows that

$$\begin{aligned} &\sum_{\vec{z} \in \mathfrak{B}(n)} e\left(\left(\frac{a}{q} + \beta\right) F(\vec{z})\right) \\ &= \sum_{\vec{b} \in \check{\mathbf{R}}_{\mathfrak{q}}} e\left(\frac{a}{q} F(\vec{b})\right) \left( \frac{1}{\mathfrak{q}^{1+k_1+k_2}} I(\beta) + O\left(\frac{n^{2+1/k_0-1/k+v}}{\mathfrak{q}^{k_1+k_2}}\right) \right) \\ &= \frac{|\check{\mathbf{R}}_{Q/\kappa(q)}|}{(Q/\kappa(q))^{1+k_1+k_2}} \frac{\check{S}_{a,q}}{q^{1+k_1+k_2}} I(\beta) + O\left(|\check{\mathbf{R}}_{\mathfrak{q}}| \frac{n^{2+1/k_0-1/k+v}}{\mathfrak{q}^{k_1+k_2}}\right) \\ &= \frac{|\check{\mathbf{R}}_{Q/\kappa(q)}|}{Q^{1+k_1+k_2}} \frac{\kappa(q)^{1+k_1+k_2}}{|\check{\mathbf{R}}_{\kappa(q)}|} \frac{\check{S}_{a,q}}{q^{1+k_1+k_2}} I(\beta) + O(\mathfrak{q} n^{2+1/k_0-1/k+v}) \end{aligned}$$

and the lemma follows.  $\square$

We introduce typical notations for the major arcs now. Compared to the classical ones, the singular series contains some additional terms in its summands as we use the restricted sum over  $\vec{z} \in \mathfrak{B}(n)$ .

$$\begin{aligned}\check{A}_n(q) &= \sum_{a \bmod^+ q} \frac{\check{S}_{a,q}}{q^{1+k_1+k_2}} e\left(-\frac{a}{q}n\right), & \check{\mathfrak{S}}(X, n) &= \sum_{q \leq X} \frac{\kappa(q)^{1+k_1+k_2}}{|\check{R}_{\kappa(q)}|} \check{A}_n(q) \\ \check{\chi}_n(p) &= \sum_{l=0}^{\infty} \frac{\kappa(p^l)^{1+k_1+k_2}}{|\check{R}_{\kappa(p^l)}|} \check{A}_n(p^l).\end{aligned}$$

In particular  $\check{A}_n(1) = 1$ . Possible issues on the convergence of  $\check{\chi}_n(p)$  will be clarified later. We also define the singular integral

$$\mathfrak{I}(c) = \int_{-c}^c \int_{\mathfrak{B}} e(\gamma F(\vec{\zeta})) d\vec{\zeta} e(-\gamma) d\gamma.$$

THEOREM 3.2.

$$\begin{aligned}& \int_{\mathfrak{M}} \sum_{\vec{z} \in \mathfrak{B}(n)} e(\alpha F(\vec{z})) e(-n\alpha) d\alpha \\ &= \frac{|\check{R}_Q|}{Q^{1+k_1+k_2}} \check{\mathfrak{S}}(n^v, n) \mathfrak{I}(n^v) n^{1+1/k_0} + O(n^{1+1/k_0-1/k+5v}).\end{aligned}\quad (3.1)$$

PROOF. Let  $\mathfrak{I}(c, n) = \int_{-c}^c I(\beta) e(-n\beta) d\beta$ . Note that there are  $O(n^{2v})$  pairs  $(q, a)$  in the major arcs and each interval  $\mathfrak{M}_{(q,a)}$  is of length  $2n^{v-1}$ . From Lemma 3.1,

$$\begin{aligned}& \sum_{q \leq n^v} \sum_{a \bmod^+ q} \int_{\mathfrak{M}_{(q,a)}} \sum_{\vec{z} \in \mathfrak{B}(n)} e(\alpha F(\vec{z})) e(-n\alpha) d\alpha \\ &= \sum_{q \leq n^v} \sum_{a \bmod^+ q} \frac{|\check{R}_Q|}{Q^{1+k_1+k_2}} \frac{\kappa(q)^{1+k_1+k_2}}{|\check{R}_{\kappa(q)}|} \frac{\check{S}_{a,q}}{q^{1+k_1+k_2}} e\left(-\frac{a}{q}n\right) \mathfrak{I}(n^{v-1}, n) \\ &\quad + O(n^{2v} n^{v-1} n^{2+1/k_0-1/k+2v}) \\ &= \frac{|\check{R}_Q|}{Q^{1+k_1+k_2}} \check{\mathfrak{S}}(n^v, n) \mathfrak{I}(n^{v-1}, n) + O(n^{1+1/k_0-1/k+5v}).\end{aligned}$$

Put  $\vec{r} = (X_0\zeta_0, X_1\zeta_1, \dots, X_1\zeta_{k_1}, X_2\zeta_{k_1+1}, \dots, X_2\zeta_{k_1+k_2})$  and  $\gamma = n\beta$  so that  $\beta F(\vec{r}) = \gamma F(\vec{\zeta})$ . Then

$$\begin{aligned}
\mathfrak{I}(n^{v-1}, n) &= \int_{-n^{v-1}}^{n^{v-1}} \int_{X_0 \mathfrak{B}_0 \times X_1 \mathfrak{B}_1 \times X_2 \mathfrak{B}_2} e(\beta F(\vec{r})) d\vec{r} e(-n\beta) d\beta \\
&= \int_{-n^v}^{n^v} X_0 X_1^{k_1} X_2^{k_2} \int_{\mathfrak{B}} e(\gamma F(\vec{\zeta})) d\vec{\zeta} e(-\gamma) \frac{d\gamma}{n} \\
&= \mathfrak{I}(n^v) n^{1+1/k_0}
\end{aligned}$$

and (3.1) follows.  $\square$

#### 4. The singular series: Bad primes

LEMMA 4.1. *If  $(q, r) = (a, q) = (b, r) = 1$  then  $\check{S}_{a,q} \check{S}_{b,r} = \check{S}_{ar+bq, qr}$ .*

PROOF. Write  $\vec{z} = (z_0, \vec{x}, \vec{y})$  and  $\vec{\zeta} = (\zeta_0, \vec{\alpha}, \vec{\beta})$ .

$$\begin{aligned}
&\sum_{\vec{z} \in \check{R}_q} e\left(\frac{a}{q} F(\vec{z})\right) \sum_{\vec{\zeta} \in \check{R}_r} e\left(\frac{b}{r} F(\vec{\zeta})\right) \\
&= \sum_{\vec{z} \in \check{R}_q} \sum_{\vec{\zeta} \in \check{R}_r} e\left(\frac{a}{q} F(\vec{z}) + \frac{b}{r} F(\vec{\zeta})\right) \\
&= \sum_{z_0=1}^q \sum_{\zeta_0=1}^r \sum_{\vec{x} \in \check{R}_q^K} \sum_{\vec{\alpha} \in \check{R}_r^K} \sum_{\vec{y} \in \check{R}_q^E} \sum_{\vec{\beta} \in \check{R}_r^E} e\left(\frac{a}{q} F(\vec{z}) + \frac{b}{r} F(\vec{\zeta})\right).
\end{aligned}$$

Let  $s_0 = rz_0 + q\zeta_0$  so that  $s_0$  takes every value modulo  $qr$ . Since  $q \in O_K$  is a unit modulo  $rO_K$ , for any  $\vec{\alpha} \in \check{R}_r^K$  one has  $N_K(q\vec{\alpha}) \not\equiv 0 \pmod{p}$  for all  $p \in \check{P}$  that divides  $r$ , i.e.,  $q\vec{\alpha} \equiv \check{R}_r^K$ . Because the map  $\vec{\alpha} \cdot \vec{\varphi} \mapsto q\vec{\alpha} \cdot \vec{\varphi}$  gives a bijection between systems of representatives of  $O_K$  modulo  $rO_K$ , we obtain a bijection  $q\check{R}_r^K \rightarrow \check{R}_r^K$ . In the same manner, the set

$$\{\vec{u} = r\vec{x} + q\vec{\alpha} : \vec{x} \in \check{R}_q^K, \vec{\alpha} \in \check{R}_r^K\}$$

is bijective to  $\check{R}_{qr}^K$  and so is

$$\{\vec{v} = r\vec{y} + q\vec{\beta} : \vec{y} \in \check{R}_q^E, \vec{\beta} \in \check{R}_r^E\}$$

to  $\check{R}_{qr}^E$ . Therefore



$$\begin{aligned}
& \sum_{z_0=1}^q \sum_{\xi_0=1}^r \sum_{\vec{x} \in \check{R}_q^K} \sum_{\vec{a} \in \check{R}_r^K} \sum_{\vec{y} \in \check{R}_q^E} \sum_{\vec{\beta} \in \check{R}_r^E} e\left(\frac{a}{q}F(\vec{z}) + \frac{b}{r}F(\vec{\xi})\right) \\
&= \sum_{z_0=1}^q \sum_{\xi_0=1}^r e\left(\frac{a}{q}s_0^{k_0} + \frac{b}{r}s_0^{k_0}\right) \sum_{\vec{x} \in \check{R}_q^K} \sum_{\vec{a} \in \check{R}_r^K} e\left(\frac{a}{q}N_K(\vec{u}) + \frac{b}{r}N_K(\vec{u})\right) \\
& \quad \sum_{\vec{y} \in \check{R}_q^E} \sum_{\vec{\beta} \in \check{R}_r^E} e\left(\frac{a}{q}N_E(\vec{v}) + \frac{b}{r}N_E(\vec{v})\right),
\end{aligned}$$

which is  $\sum_{\vec{s} \in \check{R}_{qr}} e\left(\frac{ar+bq}{qr}F(\vec{s})\right) = \check{S}_{ar+bq, qr}$ . □

An immediate implication of Lemma 4.1 is the following.

**COROLLARY 4.2.** *If  $(q, r) = 1$ , then  $\check{A}_n(q)\check{A}_n(r) = \check{A}_n(qr)$ .*

Observe that we obviously have  $\frac{\kappa(q)^{1+k_1+k_2}}{|\check{R}_{\kappa(q)}|} \frac{\kappa(r)^{1+k_1+k_2}}{|\check{R}_{\kappa(r)}|} = \frac{\kappa(qr)^{1+k_1+k_2}}{|\check{R}_{\kappa(qr)}|}$  for  $(q, r) = 1$ . Hence if we assume the convergence of  $\lim_{t \rightarrow \infty} \check{\mathfrak{S}}(t, n) = \check{\mathfrak{S}}(\infty, n)$  which will be established later, we get

$$\check{\mathfrak{S}}(\infty, n) = \prod_{p \in \mathbf{P}} \check{\chi}_n(p).$$

Let  $\check{M}_n(q)$  be the number of solutions to  $F(\vec{z}) \equiv n \pmod{q}$  with  $\vec{z} \in \check{R}_q$ .

**LEMMA 4.3.** *For  $L \geq 1$*

$$\frac{\check{M}_n(p^L)}{p^{(k_1+k_2)L}} = \frac{|\check{R}_p|}{p^{1+k_1+k_2}} + \check{A}_n(p) + \check{A}_n(p^2) + \cdots + \check{A}_n(p^L).$$

**PROOF.** Let  $q = p^L$ . It is obvious that  $\check{R}_{p^m}$  can be constructed from  $\check{R}_p$  for any  $m \geq 1$ , namely

$$\check{R}_{p^m} := \{\vec{z} \bmod p^m : \vec{z} \equiv \check{R}_p\}$$

so that  $\frac{|\check{R}_{p^m}|}{p^{m(1+k_1+k_2)}} = \frac{|\check{R}_p|}{p^{1+k_1+k_2}}$ . For  $d = (a, q) = p^l$ ,  $l \leq L$ , write

$$\check{S}_{a/d-d, q/d-d} = \sum_{\vec{z} \in \check{R}_q} e\left(\frac{a/d}{q/d}F(\vec{z})\right) = \begin{cases} d^{1+k_1+k_2} \check{S}_{a/d, q/d} & \text{if } d \neq q \\ |\check{R}_q| & \text{if } d = q. \end{cases}$$

It follows that

$$\begin{aligned}
\check{M}_n(q) &= \sum_{\vec{z} \in \check{R}_q} \frac{1}{q} \sum_{a=1}^q e\left(\frac{a}{q}(F(\vec{z}) - n)\right) \\
&= \frac{1}{q} \sum_{d|q} \sum_{\substack{a=1 \\ (a,q)=d}}^q \check{S}_{a/d \cdot d, q/d \cdot d} e\left(-\frac{a/d}{q/d} n\right) \\
&= \frac{1}{q} \left( \sum_{l=0}^{L-1} \sum_{\substack{a=1 \\ (a,q)=p^l}}^q p^{l(1+k_1+k_2)} \check{S}_{a/p^l, p^{L-l}} e\left(-\frac{a/p^l}{p^{L-l}} n\right) + |\check{R}_q| \right) \\
&= q^{k_1+k_2} \left( \sum_{l=0}^{L-1} \sum_{\substack{a=1 \\ (a,q)=p^l}}^q \frac{\check{S}_{a/p^l, p^{L-l}}}{(p^{L-l})^{1+k_1+k_2}} e\left(-\frac{a/p^l}{p^{L-l}} n\right) + \frac{|\check{R}_q|}{q^{1+k_1+k_2}} \right) \\
&= q^{k_1+k_2} \left( \sum_{l=1}^L \sum_{a \bmod^* p^l} \frac{\check{S}_{a, p^l}}{p^{l(1+k_1+k_2)}} e\left(-\frac{a}{p^l} n\right) + \frac{|\check{R}_q|}{q^{1+k_1+k_2}} \right) \\
&= q^{k_1+k_2} \left( \frac{|\check{R}_p|}{p^{1+k_1+k_2}} + \check{A}_n(p) + \check{A}_n(p^2) + \cdots + \check{A}_n(p^L) \right). \quad \square
\end{aligned}$$

The estimation of  $\check{A}_n(p^L)$  for  $p \in \check{\mathbf{P}}$  uses next lemma.

**LEMMA 4.4.** *Let  $f(\vec{z})$  be an integral polynomial in  $t+1$  variables for which  $\vec{\zeta} = (\zeta_0, \zeta_1, \dots, \zeta_t)$  is a solution to  $f(\vec{z}) \equiv n \pmod{p^M}$ . Assume that there is an  $i$  such that  $u_i = v_p\left(\frac{\partial f(\vec{z})}{\partial z_i} \Big|_{\vec{z}=\vec{\zeta}}\right) \leq \frac{M-1}{2}$ . Let  $N_i(M)$  be the number of solutions  $\vec{\xi}$  modulo  $p^M$  such that  $\xi_j \equiv \zeta_j \pmod{p^{2u_i+1}}$  for  $j \neq i$ ,  $\xi_i \equiv \zeta_i \pmod{p^{u_i+1}}$  and  $f(\vec{\xi}) \equiv n \pmod{p^M}$ . Then  $N_i(M) = p^{t(M-2u_i-1)+u_i}$ .*

**PROOF.** Without loss of generality, assume  $i = 0$  and let  $A_0 = \frac{\partial f(\vec{z})}{\partial z_0} \Big|_{\vec{z}=\vec{\zeta}}$ ,  $A_0(a, b, c, \dots) = \frac{\partial f(\vec{z})}{\partial z_0} \Big|_{\vec{z}=(\zeta_0+p^{u_0+1}a+p^{u_0+2}b+\dots, \zeta_1, \dots, \zeta_t)}$ . Note that

$$v_p(A_0(a, b, c, \dots)) = u_0$$

for all  $a, b, c, \dots \in \mathbf{Z}$ . The Hensel's lemma can be applied to this situation in a form that starts from a higher power of  $p$ :

$$\begin{aligned}
f(\zeta_0 + p^{u_0+1}z_0, \zeta_1, \dots, \zeta_t) &\equiv f(\vec{\zeta}) + A_0 p^{u_0+1}z_0 \pmod{p^{2u_0+2}}, \\
f(\zeta_0 + p^{u_0+1}z_0 + p^{u_0+2}z'_0, \zeta_1, \dots, \zeta_t) \\
&\equiv f(\zeta_0 + p^{u_0+1}z_0, \zeta_1, \dots, \zeta_t) + A_0(z_0) p^{u_0+2}z'_0 \pmod{p^{2u_0+3}},
\end{aligned}$$

and this process goes on. Thus for any  $\xi_1, \dots, \xi_t$  modulo  $p^M$  with  $\xi_j \equiv \zeta_j \pmod{p^{2u_0+1}}$ , there exists a unique  $r$  modulo  $p^{M-2u_0-1}$  such that

$$f(\zeta_0 + p^{u_0+1}r, \xi_1, \dots, \xi_t) \equiv n \pmod{p^M}.$$

Observe that this  $r$  can be lifted to a number modulo  $p^{M-u_0-1}$  in  $p^{u_0}$  distinct ways. The value of  $N_0(M)$  easily follows by counting the choices of  $\xi_1, \dots, \xi_t$  and  $\zeta_0 + p^{u_0+1}r$  modulo  $p^M$ .  $\square$

Let  $\gamma = \gamma(p) = \min\{v_p(k_1), v_p(k_2)\}$ .

LEMMA 4.5. *If  $p \in \check{\mathbf{P}}$  then  $\check{A}_n(p^L) = 0$  for all  $L > 2\gamma + 1$ .*

PROOF. Note that  $p^{(k_1+k_2)L} \check{A}(p^L) = \check{M}_n(p^L) - p^{k_1+k_2} \check{M}_n(p^{L-1})$  for  $L \geq 2$ . We show that all of the solutions that are counted in  $\check{M}_n(p^L)$  and  $\check{M}_n(p^{L-1})$  cancel out if  $L \geq 2\gamma + 2$ . Assume  $\gamma = v_p(k_1)$ . Suppose  $\vec{z} = (z_0, \vec{x}, \vec{y}) \in \check{R}_{p^m}$  is a solution counted in  $\check{M}_n(p^m)$  where  $p \in \check{\mathbf{P}}$ . Let  $G = \text{Gal}(K|\mathbf{Q})$ . Then  $N_K(\vec{x}) = \prod_{\sigma \in G} (x_1 \varphi_1^\sigma + \dots + x_{k_1} \varphi_{k_1}^\sigma)$ , and we have

$$\begin{aligned} \frac{\partial N_K(\vec{x})}{\partial x_i} &= \sum_{\sigma \in G} \varphi_i^\sigma \prod_{\substack{\tau \in G \\ \tau \neq \sigma}} (x_1 \varphi_1^\tau + \dots + x_{k_1} \varphi_{k_1}^\tau) \\ &= \text{Tr}_{K|\mathbf{Q}} \left( \varphi_i \prod_{\substack{\sigma \in G \\ \sigma \neq \text{id}}} (x_1 \varphi_1^\sigma + \dots + x_{k_1} \varphi_{k_1}^\sigma) \right) \\ &= N_K(\vec{x}) \text{Tr}_{K|\mathbf{Q}} \left( \frac{\varphi_i}{x_1 \varphi_1 + \dots + x_{k_1} \varphi_{k_1}} \right). \end{aligned}$$

Hence

$$x_1 \frac{\partial N_K(\vec{x})}{\partial x_1} + \dots + x_{k_1} \frac{\partial N_K(\vec{x})}{\partial x_{k_1}} = N_K(\vec{x}) \text{Tr}_{K|\mathbf{Q}}(1) = k_1 N_K(\vec{x}).$$

But  $\vec{x} \in \check{R}_{p^m}^K$ , i.e.,  $N_K(\vec{x}) \not\equiv 0 \pmod{p}$  which implies  $x_i \frac{\partial N_K(\vec{x})}{\partial x_i} \not\equiv 0 \pmod{p^{\gamma+1}}$  for some  $i$ . As described in the proof of Lemma 4.4, this solution  $\vec{z}$  is one of the lifts of  $\vec{\zeta} \in \check{R}_{p^{2\gamma+1}}$  when  $m \geq 2\gamma + 1$  and so the solutions  $\vec{z} \in \check{R}_{p^L}$  and  $\vec{z}' \in \check{R}_{p^{L-1}}$  that are counted in  $\check{M}_n(p^L)$  and  $\check{M}_n(p^{L-1})$  are all lifts of the solutions  $\vec{z} \in \check{R}_{p^{2\gamma+1}}$ . Lemma 4.4 shows that the number of such lifts grows by a factor of  $p^{k_1+k_2}$  for each increment of  $m$  in the modulus  $p^m$  for  $m \geq 2\gamma + 1$ . Thus all of them are canceled in  $\check{M}_n(p^L) - p^{k_1+k_2} \check{M}_n(p^{L-1})$ .  $\square$

The estimation of  $\check{A}_n(p^L)$  for  $p \notin \check{\mathbf{P}}$  is a bit more complicated. Contrary to the classical problems in additive number theory for which the exponential sum  $S_{a,p^L}$  splits into the product of many exponential sums over single variable,  $S_{a,p^L}^K$  does not behave in the same way because  $N_K(\vec{x})$  has many off-diagonal terms of the form  $x_1^{a_1} x_2^{a_2} \dots x_k^{a_k}$ . Instead of obtaining a bound of exponential sums over a single variable, therefore, we focus on the properties of the norm map  $N_{K|\mathbf{Q}}$  and it is here that the class field theory plays a role. A successful bound for  $S_{a,p^L}^K$  comes in following sections.

## 5. Algebraic preparation for the singular series

For the estimation of the exponential sum  $S_{a,q}$ , we translate the summands  $\vec{x}$  in  $S_{a,p^L}^K$  to a system of well-chosen representatives of the quotient ring  $O_K/p^L O_K$ .

LEMMA 5.1. *Let  $e, f, g$  be the ramification index, inertial degree and decomposition number of  $p$  in  $K|\mathbf{Q}$  and write  $pO_K = \mathfrak{p}_1^e \mathfrak{p}_2^e \dots \mathfrak{p}_g^e$ . Let*

$$\alpha^{(m)} \in \left( \prod_{\substack{i=1 \\ i \neq m}}^g \mathfrak{p}_i^{eL} \right) \setminus \mathfrak{p}_m$$

*and for each  $m$  with  $1 \leq m \leq g$ , let  $\{r_1^{(m)}, r_2^{(m)}, \dots, r_{p^{efL}}^{(m)}\}$  be a system of representatives of  $O_K$  modulo  $\mathfrak{p}_m^{eL}$ . Then*

$$S_{a,p^L}^K = \sum_{i_1=1}^{p^{efL}} \dots \sum_{i_g=1}^{p^{efL}} e \left( \frac{a}{q} N_{K|\mathbf{Q}}(\alpha^{(1)} r_{i_1}^{(1)} + \dots + \alpha^{(g)} r_{i_g}^{(g)}) \right).$$

PROOF. Let  $G = \text{Gal}(K|\mathbf{Q})$ . We first recall that  $N_K(\vec{x}) \in \mathbf{Z}[x_1, \dots, x_{k_1}]$ . Indeed, the coefficient of each term  $x_1^{a_1} \dots x_{k_1}^{a_{k_1}}$  in  $N_K(\vec{x}) = \prod_{\sigma \in G} (x_1 \phi_1^\sigma + \dots + x_{k_1} \phi_{k_1}^\sigma)$  is an algebraic integer which is invariant under every  $\sigma \in G$ , so it is a rational integer. Hence for any integral vector  $\vec{v}$  that is congruent to  $\vec{x}$  modulo  $p^L$  one has  $N_K(\vec{v}) \equiv N_K(\vec{x}) \pmod{p^L}$ . Since  $x_1 \phi_1 + \dots + x_{k_1} \phi_{k_1} \equiv v_1 \phi_1 + \dots + v_{k_1} \phi_{k_1} \pmod{p^L O_K}$  if and only if  $x_i \equiv v_i \pmod{p^L}$  for all  $i$ , clearly

$$S_{a,p^L}^K = \sum_{\gamma \in \mathcal{R}} e \left( \frac{a}{p^L} N_{K|\mathbf{Q}}(\gamma) \right)$$

for any system  $\mathcal{R}$  of representatives of  $O_K/p^L O_K$ .

We may work on a more general situation like the following. Let  $I, J$  be integral ideals of  $O_K$  that are relatively prime and  $q, r$  be their absolute

norms. Note that  $q, r$  need not be relatively prime. Let  $\{t_1, \dots, t_q\}$  and  $\{u_1, \dots, u_r\}$  be systems of representatives of  $O_K/I$  and  $O_K/J$ . Suppose we put  $v_{i,j} = \beta t_i + \alpha u_j$  for some  $\alpha \in I, \beta \in J$ . Then  $v_{i,j} \equiv \beta t_i \pmod{I}$ , and hence  $v_{i,j} \equiv v_{i',j'} \pmod{I} \Leftrightarrow \beta(t_i - t_{i'}) \in I$ . If  $\beta + I$  is not a zero divisor of  $O_K/I$ , this is equivalent to  $t_i \equiv t_{i'} \pmod{I}$ . Thus  $v_{i,j}$  for  $1 \leq i \leq q, 1 \leq j \leq r$  form a system of representatives of  $O_K/IJ$  if and only if  $\beta + I$  and  $\alpha + J$  are not zero divisors in  $O_K/I$  and  $O_K/J$  respectively.

Because  $I$  and  $J$  are relatively prime,  $I + J = O_K$  and there exist  $\alpha \in I$  and  $\beta \in J$  such that  $\alpha \equiv 1 \pmod{J}$  and  $\beta \equiv 1 \pmod{I}$ .  $1 + I$  is clearly a unit in  $O_K/I$  (in particular, not a zero divisor). The existence of  $\alpha, \beta$  that satisfies the conditions mentioned above follows from this.

As an obvious generalization, assume  $I^{(1)}, \dots, I^{(g)}$  are integral ideals that are relatively prime and let  $v_m = N(I^{(m)})$ . If  $\{r_1^{(m)}, r_2^{(m)}, \dots, r_{v_m}^{(m)}\}$  is a system of representatives of  $O_K/I^{(m)}$ , there exist  $\alpha^{(1)}, \dots, \alpha^{(g)}$  with  $\alpha^{(m)} \in \prod_{i \neq m}^g I^{(i)}$  for which  $\alpha^{(m)} + I^{(m)}$  is not a zero divisor in  $O_K/I^{(m)}$  for all  $m$ . Writing  $v_{i_1, \dots, i_g} = \alpha^{(1)} r_{i_1}^{(1)} + \dots + \alpha^{(g)} r_{i_g}^{(g)}$ , the set

$$\{v_{i_1, \dots, i_g} : 1 \leq i_1 \leq v_1, \dots, 1 \leq i_g \leq v_g\}$$

forms a system of representatives of  $O_K/I^{(1)} \dots I^{(g)}$ . With the substitution  $I^{(m)} = \mathfrak{p}_m^{eL}$  and the choice of  $\alpha^{(m)}$  as stated in the lemma,  $\alpha^{(m)}$  is trivially not a zero divisor of  $O_K/\mathfrak{p}_m^{eL}$ . This completes the proof.  $\square$

The following is a well-known fact in algebraic number theory (for example, see Chapter 8 of [7].)

**PROPOSITION 5.2.** *Let  $\mathfrak{p}$  be a nonzero prime ideal of  $O_K$  and  $m \geq 1$ . Let  $\Gamma$  be a system of representatives of  $O_K$  modulo  $\mathfrak{p}$  containing 0. Let  $t \in \mathfrak{p} \setminus \mathfrak{p}^2$ . Then  $\Delta = \{s_0 + s_1 t + \dots + s_{m-1} t^{m-1} : s_i \in \Gamma\}$  is a system of representatives of  $O_K$  modulo  $\mathfrak{p}^m$ .*

Let  $e, f, g$  be as in Lemma 5.1. We want to choose a system of representatives of  $O_K$  modulo  $\mathfrak{p}_m^{eL}$  in a nice way. Consider the ideal class group  $\mathcal{C}$  of  $K$  and a class  $[I] \in \mathcal{C}$  containing  $I$ . An analogue of Dirichlet's theorem on primes in arithmetic progression is that the prime ideals of  $O_K$  are equi-distributed among ideal classes in  $\mathcal{C}$  on a probabilistic point of view (Chapter 11 of [5]). We simply take a weaker form of this for granted that every ideal class contains infinitely many prime ideals.

Firstly, consider  $[\mathfrak{p}_1] \in \mathcal{C}$ . Then there is a prime ideal  $\mathfrak{a}_1$  such that  $[\mathfrak{a}_1] = [\mathfrak{p}_1]^{-1}$  in  $\mathcal{C}$  and  $\gcd(\mathfrak{a}_1, \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_g) = O_K$ . Now  $\mathfrak{p}_1 \mathfrak{a}_1$  is principal, say,  $t O_K$  and for  $m \neq 1$

$$\begin{aligned}
\left( \left( \prod_{\substack{i=1 \\ i \neq m}}^g \mathfrak{p}_i^{eL} \right) \setminus \mathfrak{p}_m \right) \cap t^{eL} O_K &= lcm \left( \prod_{\substack{i=1 \\ i \neq m}}^g \mathfrak{p}_i^{eL}, t^{eL} O_K \right) \setminus \mathfrak{p}_m \\
&= \left( \alpha_1^{eL} \prod_{\substack{i=1 \\ i \neq m}}^g \mathfrak{p}_i^{eL} \right) \setminus \mathfrak{p}_m \\
&\neq \emptyset
\end{aligned}$$

whence one can choose  $\alpha^{(m)} \in (\alpha_1^{eL} \prod_{\substack{i=1 \\ i \neq m}}^g \mathfrak{p}_i^{eL}) \setminus \mathfrak{p}_m$ , i.e.,  $\alpha^{(m)} \in \alpha_1^{eL} \mathfrak{p}_1^{eL} = t^{eL} O_K$  and  $\alpha^{(m)} / t^{eL} \in O_K$  for  $m = 2, 3, \dots, g$ .

Similarly, we can choose  $\alpha_1, \alpha_2, \dots, \alpha_g$  so that  $\mathfrak{p}_i \alpha_i = t_i O_K$  is principal and  $\gcd(\alpha_i, \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_g) = O_K$  for all  $i$ . In particular  $t_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$  and  $v_p(N_{K|\mathbf{Q}}(t_i)) = f$ . By the infinitude of the prime ideals in every ideal class, we can in addition assume  $(\alpha_i, \alpha_j) = O_K$  for  $i \neq j$ . It follows that there exists an element

$$\alpha^{(m)} \in \left( \prod_{\substack{i=1 \\ i \neq m}}^g \alpha_i^{eL} \mathfrak{p}_i^{eL} \right) \setminus \mathfrak{p}_m$$

for each  $m$  so that

$$\frac{\alpha^{(m)}}{\prod_{\substack{i=1 \\ i \neq m}}^g t_i^{eL}} \in O_K \setminus \mathfrak{p}_m.$$

Let  $\Gamma^{(1)}, \dots, \Gamma^{(g)}$  be systems of representatives of  $O_K / \mathfrak{p}_1, \dots, O_K / \mathfrak{p}_g$  that contain 0. In the estimation of  $S_{a, p^L}^K$  later, we choose the representatives that are of the form

$$\sum_{m=1}^g \alpha^{(m)} (s_0^{(m)} + s_1^{(m)} t_m + s_2^{(m)} t_m^2 + \dots + s_{eL-1}^{(m)} t_m^{eL-1}) \quad (5.1)$$

where  $s_j^{(m)} \in \Gamma^{(m)}$ .

## 6. The singular series: Good primes

Let  $\mathcal{R}$  be a system of representatives of  $O_K / p^L O_K$  and  $\mathcal{R}^* = \{r \in \mathcal{R} : p \nmid N_{K|\mathbf{Q}}(r)\}$ . Let  $e, f, g$  be as in Lemma 5.1. Note that  $\check{S}_{a, p^L}^K = S_{a, p^L}^K$  if  $p \notin \mathbf{P}$ .

LEMMA 6.1. Write  $S_{a,p^L}^K = S_{a,p^L}^{K,1} + S_{a,p^L}^{K,2}$  where

$$S_{a,p^L}^{K,1} = \sum_{\gamma \in \mathcal{R}^*} e\left(\frac{a}{p^L} N_{K|\mathbf{Q}}(\gamma)\right), \quad S_{a,p^L}^{K,2} = \sum_{\gamma \in \mathcal{R} \setminus \mathcal{R}^*} e\left(\frac{a}{p^L} N_{K|\mathbf{Q}}(\gamma)\right).$$

- (1) If  $L \leq f$  then  $S_{a,p^L}^{K,2} = \sum_{i=1}^g (-1)^{i-1} \binom{g}{i} p^{k_1 L - if}$
- (2) If  $L > 1$  and  $p \nmid k_1$  then  $S_{a,p^L}^{K,1} = 0$
- (3) If  $L = 1$  and  $p$  is unramified in  $K|\mathbf{Q}$  then  $S_{a,p^L}^{K,1} = -\frac{(p^f - 1)^g}{p - 1}$ .

PROOF. Assume  $L \leq f$ . Since  $p \mid N_{K|\mathbf{Q}}(\gamma)$  if and only if  $p^f \mid N_{K|\mathbf{Q}}(\gamma)$ , in this case  $S_{a,p^L}^{K,2}$  merely counts the number of nonunits of  $O_K/p^L O_K = O_K/\mathfrak{p}_1^{eL} \dots \mathfrak{p}_g^{eL}$ . Let  $T$  be the number of nonunits in  $O_K/p O_K$ . The number of units in  $O_K/p O_K$  is  $(p^{ef} - p^{(e-1)f})^g$ , so

$$\begin{aligned} T &= p^{k_1} - (p^{ef} - p^{(e-1)f})^g = p^{k_1} - p^{efg}(1 - p^{-f})^g \\ &= \sum_{i=1}^g (-1)^{i-1} \binom{g}{i} p^{k_1 - if} \end{aligned}$$

and  $S_{a,p^L}^{K,2} = p^{(L-1)k_1} T = \sum_{i=1}^g (-1)^{i-1} \binom{g}{i} p^{k_1 L - if}$ .

As for  $S_{a,p^L}^{K,1}$ , first assume  $L > 1$  and  $p \nmid k_1$ . Let  $\vec{x}$  be given by  $\gamma = \vec{x} \cdot \vec{\varphi}$ . Since  $p \nmid k_1$ ,  $p \nmid N_K(\vec{x})$  implies that there exists  $i$  such that  $\frac{\partial N_K(\vec{x})}{\partial x_i} \not\equiv 0 \pmod{p}$  as shown in the proof of Lemma 4.5. If  $m$  is any integer such that  $m \equiv N_K(\vec{x}) \pmod{p}$ , Lemma 4.4 shows that the number of  $\vec{v}$  modulo  $p^{L-1}$  satisfying  $N_K(\vec{x} + p\vec{v}) \equiv m \pmod{p^L}$  is  $p^{(k_1-1)(L-1)}$ . Thus

$$S_{a,p^L}^{K,1} = p^{(k_1-1)(L-1)} \sum_{\substack{\vec{x} \bmod p \\ p \nmid N_K(\vec{x})}} \sum_{z=1}^{p^{L-1}} e\left(\frac{a}{p^L} (N_K(\vec{x}) + pz)\right) = 0.$$

Now assume  $L = 1$  and  $p$  is unramified in  $K|\mathbf{Q}$  so that  $N_{K|\mathbf{Q}}(r)$  takes every nonzero value modulo  $p$ . Considering  $N_{K|\mathbf{Q}}(ru)$  for  $u \in \mathcal{R}^*$ , it is easy to see that the number of  $r \in \mathcal{R}^*$  satisfying  $N_{K|\mathbf{Q}}(r) \equiv m \pmod{p}$  is the same for each value of  $m = 1, 2, \dots, p-1$ . It follows that

$$\begin{aligned} \sum_{r \in \mathcal{R}^*} e\left(\frac{a}{p} N_{K|\mathbf{Q}}(r)\right) &= \frac{(p^{ef} - p^{(e-1)f})^g}{p-1} \sum_{m=1}^{p-1} e\left(\frac{a}{p} m\right) \\ &= -p^{k_1 - fg} \frac{(p^f - 1)^g}{p-1} = -\frac{(p^f - 1)^g}{p-1}. \quad \square \end{aligned}$$

We include a classical bound of an exponential sum for convenience. Let  $S_{a,q}^0 = \sum_{m=1}^q e\left(\frac{a}{q} m^{k_0}\right)$ .

LEMMA 6.2 (Theorem 4.2 of [8]). For  $(a, q) = 1$ ,  $S_{a, q}^0 \ll q^{1-1/k_0}$ .

Let  $e, f, g$  be as in Lemma 5.1,  $t_1, \dots, t_g$  and  $\alpha^{(1)}, \dots, \alpha^{(g)}$  as described in Section 5. Choose a system  $\mathcal{R}$  of representatives of  $O_K/p^L O_K$  whose elements are of the form given by (5.1).

LEMMA 6.3. Let  $p \notin \check{\mathbf{P}}$ . For  $L \geq 1$ ,

$$|S_{a, p^L}^K| \ll (p^L)^{k_1-1+2 \log_p k_1} \quad \text{and} \quad |S_{a, p^L}^E| \ll (p^L)^{k_2-1+2 \log_p k_2}.$$

PROOF. We prove the first inequality. Write  $L = uf + v$ ,  $1 \leq v \leq f$  and let  $\mathcal{R}_i = \{r \in \mathcal{R} : r \in \mathfrak{p}_i\}$ . The case  $L = 1$  easily follows from Lemmas 6.1 and 6.2, so we assume  $L > 1$ . Since  $p \nmid k_1$ , by Lemma 6.1 and the inclusion-exclusion principle

$$\begin{aligned} S_{a, p^L}^K &= S_{a, p^L}^{K, 2} = \sum_{r \in \bigcup_{m=1}^g \mathcal{R}_m} e\left(\frac{a}{p^{L-f}} \frac{N_{K|\mathbf{Q}}(r)}{p^f}\right) \\ &= \sum_{l=1}^g (-1)^{l-1} \sum_{\substack{i_1, \dots, i_l=1 \\ i_1 < \dots < i_l}}^g \sum_{r \in \bigcap_{m=1}^l \mathcal{R}_{i_m}} E(i_1, \dots, i_l) \\ &= \sum_1 + \sum_2 \end{aligned}$$

where

$$E(i_1, \dots, i_l) = e\left(\frac{a}{p^{L-lf}} \frac{N_{K|\mathbf{Q}}(t_{i_1} t_{i_2} \dots t_{i_l})}{p^{lf}} N_{K|\mathbf{Q}}\left(\frac{r}{t_{i_1} t_{i_2} \dots t_{i_l}}\right)\right),$$

and, in case  $L \leq fg$ , we wrote the sum over  $l < \lfloor L/f \rfloor$  as  $\sum_1$  and the sum over  $\lfloor L/f \rfloor \leq l \leq g$  as  $\sum_2$ . Let  $a_{(i_1, \dots, i_l)} = a \frac{N_{K|\mathbf{Q}}(t_{i_1} t_{i_2} \dots t_{i_l})}{p^{lf}}$ . By the choice of  $\mathcal{R}$ , we have  $(a_{(i_1, \dots, i_l)}, p) = 1$  and  $\frac{r}{t_{i_1} t_{i_2} \dots t_{i_l}} \in O_K$  when  $r \in \bigcap_{m=1}^l \mathcal{R}_{i_m}$ . For  $\sum_1$ , observe that  $\{\frac{r}{t_{i_1} t_{i_2} \dots t_{i_l}} : r \in \bigcap_{m=1}^l \mathcal{R}_{i_m}\}$  runs through a system of representatives modulo  $p^{L-lf} O_K$  by  $p^{lfk_1-lf}$  times. As for  $\sum_2$ , we first note that  $E(i_1, \dots, i_l) = 1$  always. Recall that an element of  $\mathcal{R}$  is of the form

$$r = \sum_{m=1}^g \alpha^{(m)} (s_0^{(m)} + s_1^{(m)} t_m + s_2^{(m)} t_m^2 + \dots + s_{L-1}^{(m)} t_m^{L-1})$$

where  $s_j^{(m)} \in \Gamma^{(m)}$ ,  $|\Gamma^{(m)}| = p^f$ , and  $r \in \mathcal{R}_i$  if and only if  $s_0^{(i)} = 0$ . The set  $\bigcap_{m=1}^l \mathcal{R}_{i_m}$  consists of the numbers with  $s_0^{(i_1)} = \dots = s_0^{(i_l)} = 0$  and hence contains  $p^{lf(L-1)} p^{(g-l)fL} = p^{k_1 L - lf}$  elements. We thus can write



$$\begin{aligned}
S_{a,p^L}^K &= \sum_{\substack{1 \leq l \leq g \\ l < \lfloor L/f \rfloor}} (-1)^{l-1} \sum_{\substack{i_1, \dots, i_l=1 \\ i_1 < \dots < i_l}}^g p^{(k_1-1)lf} S_{a(i_1, \dots, i_l), p^{L-lf}}^K \\
&+ \sum_{\lfloor L/f \rfloor \leq l \leq g} (-1)^{l-1} \sum_{\substack{i_1, \dots, i_l=1 \\ i_1 < \dots < i_l}}^g p^{k_1 L - lf}.
\end{aligned}$$

Let  $M(x)$  be the maximum value of  $|S_{b,p^x}^K|$  among all  $b \not\equiv 0 \pmod{p}$  for  $x \geq 1$ , and  $p^{k_1 x}$  when  $x \leq 0$ . Let  $\theta_{(x)} = \theta_{K,p}(x)$  be the real number satisfying  $M(x) = p^{x(k_1-1+\theta_{(x)})}$ . (In particular,  $\theta_{(x)} = 1$  when  $x < 0$  and by convention we put  $\theta_{(0)} = 1$ .) Then we have

$$\begin{aligned}
|S_{a,p^L}^K| &\leq \sum_{l=1}^g \binom{g}{l} p^{lf(k_1-1)} M(L-lf) \\
&\leq g \cdot \max_l \left\{ \binom{g}{l} p^{lf(k_1-1)} M(L-lf) \right\} \\
&\leq g \cdot \max_l \left\{ \binom{g}{l} p^{lf(k_1-1)+(L-lf)(k_1-1+\theta_{(L-lf)})} \right\} \\
&\leq \max_l \{ p^{(L-lf)(k_1-1+\theta_{(L-lf)})+lf(k_1-1+\log_p g/f+\log_p g/lf)} \}
\end{aligned}$$

whence for some  $l$

$$L(k_1 - 1 + \theta_{(L)}) \leq L(k_1 - 1 + \theta_{(L-lf)}) + lf \left( -\theta_{(L-lf)} + \frac{l+1}{lf} \log_p g \right)$$

or

$$L\theta_{(L)} \leq \max_l \{ (L-lf)\theta_{(L-lf)} + (l+1) \log_p g \}.$$

From this expression, in an inductive way, one immediately has

$$(uf + v)\theta_{(uf+v)} \leq v\theta_{(v)} + 2u \log_p g. \quad (6.1)$$

Assume  $v = 1$  first. By Lemma 6.1,  $S_{a,p}^K = -\frac{(p^f-1)^g}{p-1} + \sum_{i=1}^g (-1)^{i-1} \binom{g}{i} p^{k_1-if}$ . Here

$$\begin{aligned}
\frac{(p^f-1)^g}{p-1} &= (p^{f-1} + p^{f-2} + \dots + 1)(p^f-1)^{g-1} \\
&< 2p^{f-1} p^{f(g-1)} = p^{k_1-1+\log_p 2},
\end{aligned}$$

and observe that  $0 < \sum_{i=1}^g (-1)^{i-1} \binom{g}{i} p^{k_1 - if} \leq gp^{k_1 - f}$ . Thus

$$|S_{a,p}^K| < \max\{p^{k_1 - 1 + \log_p 2}, gp^{k_1 - f}\} \leq k_1 p^{k_1 - 1} = p^{k_1 - 1 + \log_p k_1}.$$

Now assume  $v > 1$ . Then

$$|S_{a,p^v}^K| = \left| \sum_{i=1}^g (-1)^{i-1} \binom{g}{i} p^{vk_1 - if} \right| \leq k_1 p^{vk_1 - f} = p^{v(k_1 - 1 + 1 - f/v + \log_p k_1/v)}$$

and  $1 - \frac{f}{v} + \frac{\log_p k_1}{v} \leq \frac{\log_p k_1}{f}$  where the equality holds when  $v = f$ . We have proved that  $v\theta_{(v)} \leq \log_p k_1$  in both cases; hence from (6.1)

$$\theta_{(uf+v)} \leq \frac{\log_p k_1 + 2u \log_p g}{uf + v} \leq \frac{(2u+1) \log_p k_1}{u+1} < 2 \log_p k_1. \quad \square$$

The next one is an immediate corollary.

LEMMA 6.4. *If  $p \notin \check{\mathbf{P}}$  then there exists an absolute constant  $\delta > 0$  such that  $\check{A}_n(p^L) \ll \frac{1}{(p^L)^{1+\delta}}$ .*

PROOF. Since  $\check{S}_{a,p^L} = S_{a,p^L}$  for  $p \notin \check{\mathbf{P}}$ , by Lemmas 6.2 and 6.3

$$\begin{aligned} \check{A}_n(p^L) &\ll \frac{1}{(p^L)^{1+k_1+k_2}} \cdot p^L \cdot |S_{a,p^L}^0 S_{a,p^L}^K S_{a,p^L}^E| \\ &\ll p^{L(-k_1-k_2+(1-1/k_0)+(k_1-1+2\log_p k_1)+(k_2-1+2\log_p k_2))} \\ &< p^{L(-1-1/k_0+2\log_p k_1 k_2)} \end{aligned}$$

and  $2 \log_p k_1 k_2 < \frac{1}{k_0}$  because  $p \notin \check{\mathbf{P}}$ .  $\square$

Now the singular series is estimated.

THEOREM 6.5. *There exist positive absolute constants  $c_1, c_2$  that depend only on  $K$  and  $E$  such that  $c_1 < \check{\mathfrak{S}}(n^v, n) < c_2$  for all sufficiently large  $n$ .*

PROOF. Since  $1 \leq \frac{\kappa(q)^{1+k_1+k_2}}{|\check{R}_{\kappa(q)}|} \leq \frac{Q^{1+k_1+k_2}}{|\check{R}_Q|} \ll 1$ , the absolute convergence of

$$\lim_{t \rightarrow \infty} \check{\mathfrak{S}}(t, n) = \check{\mathfrak{S}}(\infty, n)$$

follows from Corollary 4.2, Lemmas 4.5 and 6.4. More precisely we have

$$|\check{\mathfrak{S}}(\infty, n) - \check{\mathfrak{S}}(n^v, n)| \ll \frac{1}{n^{v\delta}}$$

so it suffices to show that  $0 < c_1 < \check{\mathfrak{S}}(\infty, n) = \prod_{p \in \mathbf{P}} \check{\chi}_n(p) < c_2$  for some constants  $c_1$  and  $c_2$ .

For  $p \notin \check{\mathbf{P}}$ ,  $\frac{\kappa(p)^{1+k_1+k_2}}{|\check{\mathbf{R}}_{\kappa(p)}|} = 1$  so Lemma 6.4 gives

$$|\check{\chi}_n(p) - 1| \leq \sum_{L=1}^{\infty} |\check{A}_n(p^L)| \ll \sum_{L=1}^{\infty} \frac{1}{(p^L)^{1+\delta}} \ll \frac{1}{p^{1+\delta}}$$

which implies that there exists a prime  $p_0$  depending only on  $K$  and  $E$  such that

$$\frac{1}{2} < \prod_{p \geq p_0} \check{\chi}_n(p) < \frac{3}{2}.$$

Suppose  $p < p_0$ . Recall that every prime  $p$  is unramified in at least one of  $K|\mathbf{Q}$  and  $E|\mathbf{Q}$ , so assume  $p$  is unramified in  $K|\mathbf{Q}$ . For  $L \geq 2$ ,  $\check{M}_n(p^L) \geq N_n(p^L)$  where

$$N_n(p^L) = |\{\vec{z} \in \check{\mathbf{R}}_{p^L} : F(\vec{z}) \equiv n \pmod{p^L}, N_K(\vec{x}) \not\equiv 0 \pmod{p}\}|.$$

As in the proof of Lemma 6.1, the number  $s(m)$  of  $\vec{x}$  modulo  $p^L$  satisfying  $N_K(\vec{x}) \equiv m \pmod{p^L}$  is the same for all  $m \not\equiv 0 \pmod{p}$ . Since there are  $(p^f - 1)^g p^{(L-1)k_1}$  units in  $O_K/p^L O_K = \mathfrak{p}_1^L \dots \mathfrak{p}_g^L$ , it is easy to see that  $s(m) = \frac{(p^f - 1)^g p^{(L-1)k_1}}{(p-1)p^{L-1}}$ . Let  $h(L)$  be the number of  $(z_0, \vec{y})$  modulo  $p^L$  such that  $\vec{y} \in \check{\mathbf{R}}_{p^L}^E$  and  $z_0^{k_0} + N_E(\vec{y}) - n \not\equiv 0 \pmod{p}$ . For each  $\vec{y} \in \check{\mathbf{R}}_{p^L}^E$ , if  $N_E(\vec{y}) - n \equiv 0 \pmod{p}$  then there are  $p^L - p^{L-1}$   $z_0$ 's counted by  $h(L)$ . Otherwise there are at least  $p^{L-1}$   $z_0$ 's, so  $h(L) \geq |\check{\mathbf{R}}_{p^L}^E| p^{L-1} = |\check{\mathbf{R}}_p^E| p^{(L-1)(k_2+1)}$ . It follows that

$$\begin{aligned} N_n(p^L) &\geq s(1)h(L) \geq \frac{(p^f - 1)^g}{p - 1} p^{(L-1)(k_1-1) + (L-1)(k_2+1)} |\check{\mathbf{R}}_p^E| \\ &\geq (p-1)^{k_1-1} |\check{\mathbf{R}}_p^E| p^{(k_1+k_2)(L-1)}. \end{aligned}$$

Let  $e'$ ,  $f'$ ,  $g'$  be the ramification index, inertial degree and decomposition number of  $p$  in  $E|\mathbf{Q}$ . Then

$$|\check{\mathbf{R}}_p^E| \geq |(O_E/pO_E)^*| = (p^{e'f'} - p^{(e'-1)f'})^{g'} = p^{k_2} \left(1 - \frac{1}{p^{f'}}\right)^{g'} \geq \left(\frac{p}{2}\right)^{k_2},$$

and hence

$$\frac{N_n(p^L)}{p^{(k_1+k_2)L}} \geq \frac{(p-1)^{k_1-1}}{2^{k_2} p^{k_1}}.$$

Now write  $\check{\chi}_n^{(L)}(p) = \sum_{l=0}^L \frac{\kappa(p^l)^{1+k_1+k_2}}{|\check{\mathbf{R}}_{\kappa(p^l)}|} \check{A}_n(p^l)$ . By Lemma 4.3,

$$\check{\chi}_n^{(L)}(p) = \frac{\kappa(p)^{1+k_1+k_2}}{|\check{\mathbf{R}}_{\kappa(p)}|} \frac{\check{M}_n(p^L)}{p^{(k_1+k_2)L}} \geq \frac{\kappa(p)^{1+k_1+k_2}}{|\check{\mathbf{R}}_{\kappa(p)}|} \frac{(p-1)^{k_1-1}}{2^{k_2} p^{k_1}} =: u_p$$

and so  $\check{\chi}_n(p) \geq u_p > 0$ .

As for the upper bound of  $\check{\chi}_n(p)$ , if  $p \in \check{\mathbf{P}}$  then Lemmas 4.5 and 4.3 give

$$\begin{aligned}\check{\chi}_n(p) &= \sum_{l=0}^{2\gamma(p)+1} \frac{\kappa(p^l)^{1+k_1+k_2}}{|\check{R}_{\kappa(p^l)}|} \check{A}_n(p^l) = \frac{p^{1+k_1+k_2}}{|\check{R}_p|} \frac{\check{M}_n(p^{2\gamma(p)+1})}{p^{(k_1+k_2)(2\gamma(p)+1)}} \\ &\leq \frac{p^{1+k_1+k_2}}{|\check{R}_p|} \frac{|\check{R}_p| p^{(1+k_1+k_2)2\gamma(p)}}{p^{(k_1+k_2)(2\gamma(p)+1)}} = p^{2\gamma(p)+1}.\end{aligned}$$

If  $p \notin \check{\mathbf{P}}$ ,  $\check{\chi}_n(p)$  converges absolutely by Lemma 6.4. As the bound in Lemma 6.4 is independent of  $n$ , one can choose an upper bound  $U_p$  of  $\check{\chi}_n(p)$  that depends only on  $K$  and  $E$ . Therefore

$$c_1 = \frac{1}{2} \prod_{p < p_0} u_p < \check{\mathfrak{S}}(\infty, n) < \frac{3}{2} (k_1, k_2)^2 \prod_{p \in \check{\mathbf{P}}} p \prod_{\substack{p < p_0 \\ p \notin \check{\mathbf{P}}}} U_p = c_2. \quad \square$$

## 7. The singular integral and minor arcs

The following proof is basically from [4].

**THEOREM 7.1.** *We can choose  $\mathfrak{B}$  so that  $\mathfrak{I}(n^v) \rightarrow \mathfrak{I}_0 > 0$  as  $n \rightarrow \infty$ .*

**PROOF.** Choose small positive numbers  $\phi_1, \dots, \phi_{k_1+k_2}$  so that the real value  $\phi_0$  that makes  $\phi_0^{k_0} + N_K(\phi_1, \dots, \phi_{k_1}) + N_E(\phi_{k_1+1}, \dots, \phi_{k_1+k_2}) = 1$  is positive, not equal to 1, and hence

$$\partial F / \partial \phi_0 \neq 0 \quad \text{and} \quad N_K(\phi_1, \dots, \phi_{k_1}) + N_E(\phi_{k_1+1}, \dots, \phi_{k_1+k_2}) \neq 0.$$

Then  $\vec{\phi} = (\phi_0, \dots, \phi_{k_1+k_2})$  is a nonsingular solution to  $F(\vec{\phi}) = 1$ . Let  $\mathfrak{B}$  be a box centered at  $\vec{\phi}$  with side lengths  $2\lambda$ . Write

$$\begin{aligned}\mathfrak{I}(\mu) &= \int_{-\mu}^{\mu} \int_{\mathfrak{B}} e(\gamma F(\vec{\zeta})) d\vec{\zeta} e(-\gamma) d\gamma \\ &= \int_{\mathfrak{B}} \frac{\sin 2\pi\mu(F(\vec{\zeta}) - 1)}{\pi(F(\vec{\zeta}) - 1)} d\vec{\zeta} \\ &= \int_{-\lambda}^{\lambda} \dots \int_{-\lambda}^{\lambda} \frac{\sin 2\pi\mu(F(\vec{\phi} + \vec{\theta}) - 1)}{\pi(F(\vec{\phi} + \vec{\theta}) - 1)} d\vec{\theta}.\end{aligned}$$

Write  $F(\vec{\phi} + \vec{\theta}) - 1 = c_0\theta_0 + \dots + c_{k_1+k_2}\theta_{k_1+k_2} + P_2(\vec{\theta}) + \dots + P_k(\vec{\theta})$  where  $P_m(\vec{\theta})$  is a homogeneous polynomial of degree  $m$ . Note that  $c_0 = \partial F / \partial \theta_0|_{\vec{\theta}=\vec{0}} = k_0\phi_0^{k_0-1} \neq 0$ . Now for  $r_0, r_1, r_2 \in \mathbf{R}$  consider the equation

$$r_0^{k_0} \phi_0^{k_0} + r_1^{k_1} N_K(\phi_1, \dots, \phi_{k_1}) + r_2^{k_2} N_E(\phi_{k_1+1}, \dots, \phi_{k_1+k_2}) - 1 = 0.$$

Since both of  $\phi_0$  and  $N_K(\phi_1, \dots, \phi_{k_1}) + N_E(\phi_{k_1+1}, \dots, \phi_{k_1+k_2})$  are nonzero, one can choose  $r_0, r_1, r_2 > 0$  such that  $k_0(r_0\phi_0)^{k_0-1} = 1$  and still satisfying

$$F(r_0\phi_0, r_1\phi_1, \dots, r_1\phi_{k_1}, r_2\phi_{k_1+1}, \dots, r_2\phi_{k_1+k_2}) - 1 = 0 \quad \text{and}$$

$$N_K(r_1\phi_1, \dots, r_1\phi_{k_1}) + N_E(r_2\phi_{k_1+1}, \dots, r_2\phi_{k_1+k_2}) \neq 0.$$

So we can assume  $c_0 = k_0\phi_0^{k_0-1} = 1$  from the beginning.

For  $|\vec{\theta}| < \lambda$ , we have  $|F(\vec{\phi} + \vec{\theta}) - 1| < \sigma$  where  $\sigma = \sigma(\lambda)$  is small for small  $\lambda$ . Put  $F(\vec{\phi} + \vec{\theta}) - 1 = t$ , and consider this as a map from  $\theta_0$  to  $t$ . Then, if  $\lambda$  is sufficiently small, the inverse function theorem tells us that  $\theta_0$  can be expressed in terms of  $t, \theta_1, \dots, \theta_{k_1+k_2}$  as a power series

$$\theta_0 = t - c_1\theta_1 - \dots - c_{k_1+k_2}\theta_{k_1+k_2} + \mathcal{P}(t, \theta_1, \dots, \theta_{k_1+k_2})$$

where  $\mathcal{P}$  is a multiple power series whose least degree terms are of degree at least 2. Hence  $\partial\theta_0/\partial t = 1 + \mathcal{P}_1(t, \theta_1, \dots, \theta_{k_1+k_2})$  where  $\mathcal{P}_1$  is a multiple power series without a constant term. By taking  $\lambda$  sufficiently small, we can make  $|\mathcal{P}_1(t, \theta_1, \dots, \theta_{k_1+k_2})| < 1/2$  for  $|\theta_1|, \dots, |\theta_{k_1+k_2}| < \lambda$ ,  $|t| < \sigma$ . A change of variable from  $\theta_0$  to  $t$  gives

$$\begin{aligned} \mathfrak{I}(\mu) &= \int_{-\lambda}^{\lambda} \dots \int_{-\lambda}^{\lambda} \frac{\sin 2\pi\mu(F(\vec{\phi} + \vec{\theta}) - 1)}{\pi(F(\vec{\phi} + \vec{\theta}) - 1)} d\theta_1 \dots d\theta_{k_1+k_2} d\theta_0 \\ &\sim \int_{-\sigma}^{\sigma} \frac{\sin 2\pi\mu t}{\pi t} V(t) dt \end{aligned}$$

where  $V(t) = \int_{-\lambda}^{\lambda} \dots \int_{-\lambda}^{\lambda} (1 + \mathcal{P}_1(t, \theta_1, \dots, \theta_{k_1+k_2})) d\theta_1 \dots d\theta_{k_1+k_2}$  and we wrote  $a \sim b$  to mean that the limit of their ratio equals 1.

$V(t)$  is clearly a continuous function of  $t$  for  $|t|$  sufficiently small. We also observe that  $V(t)$  has left and right derivatives at every value of  $t$ , and these derivatives are certainly bounded for  $t$  in a small confined region. Therefore by Fourier integral theorem one has

$$\lim_{\mu \rightarrow \infty} \mathfrak{I}(\mu) = \lim_{\mu \rightarrow \infty} \int_{-\sigma}^{\sigma} \frac{\sin 2\pi\mu t}{\pi t} V(t) dt = V(0) =: \mathfrak{I}_0.$$

But

$$\begin{aligned} |V(0)| &= \left| \int_{-\lambda}^{\lambda} \dots \int_{-\lambda}^{\lambda} (1 + \mathcal{P}_1(0, \theta_1, \dots, \theta_{k_1+k_2})) d\theta_1 \dots d\theta_{k_1+k_2} \right| \\ &> \int_{-\lambda}^{\lambda} \dots \int_{-\lambda}^{\lambda} \frac{1}{2} d\theta_1 \dots d\theta_{k_1+k_2} > 0 \end{aligned}$$

and the theorem follows.  $\square$

We merely state the estimation on the minor arcs, which can be easily seen in [1].

**THEOREM 7.2.** *There exists  $\delta > 0$  that depends only on  $K$  and  $E$  such that*

$$\int_{\mathfrak{m}} \sum_{\vec{z} \in \mathfrak{B}(n)} e(\alpha F(\vec{z})) e(-n\alpha) d\alpha \ll n^{1+1/k_0-\delta}.$$

## 8. Conclusion

By Theorems 3.2, 6.5, 7.1 and 7.2 one has

**THEOREM 8.1.** *The number of representations,  $\check{r}(n)$ , of  $n$  in the form  $z_0^{k_0} + N_K(\vec{x}) + N_E(\vec{y})$  with  $\vec{z} = (z_0, \vec{x}, \vec{y}) \in \check{\mathfrak{B}}(n)$  satisfies*

$$\check{r}(n) = \frac{|\check{R}_Q|}{Q^{1+k_1+k_2}} \mathfrak{I}_0 \left( \prod_{p \in \mathbf{P}} \check{\chi}_n(p) \right) n^{1+1/k_0} + o(n^{1+1/k_0})$$

where  $1 \ll \mathfrak{I}_0 \prod_{p \in \mathbf{P}} \check{\chi}_n(p) \ll 1$ .

A remark can be made on this result. Theorem 8.1 is optimal in the sense that the term  $z_0^{k_0}$  is invincible to make the polynomial almost universal in any cases. We give here an example of a sum of two norms  $N_K(\vec{x}) + N_E(\vec{y})$  which is locally universal but is not almost universal. This can be summarized as follows.

Let  $f = f_{A,B}(\vec{u}) = N_{\mathbf{Q}(\sqrt{-A})|\mathbf{Q}}(u_1 + u_3\sqrt{-A}) + N_{\mathbf{Q}(\sqrt{-B})|\mathbf{Q}}(u_2 + u_4\sqrt{-B}) = u_1^2 + u_2^2 + Au_3^2 + Bu_4^2$  be a quaternary quadratic form. Choose  $A, B$  among prime numbers congruent to 1 modulo 8 that are sufficiently large so that  $f$  cannot represent all of  $\{16, 32, 48, 80, 96, 112, 160, 224\}$ . (In particular,  $48 = 2^4 \cdot 3 \neq u_1^2 + u_2^2$ ).  $f$  is locally universal, since  $N_{\mathbf{Q}(\sqrt{-A})|\mathbf{Q}}$  takes every unit value in  $\mathbf{Z}_p$  for  $p \neq 2, A$  and the same holds for  $N_{\mathbf{Q}(\sqrt{-B})|\mathbf{Q}}$  in  $\mathbf{Z}_p$  when  $p \neq 2, B$ . When  $p = 2$ , we see that  $A$  and  $B$  are in  $(\mathbf{Z}_2^*)^2$  and  $f$  is equivalent to  $u_1^2 + u_2^2 + u_3^2 + u_4^2$  over  $\mathbf{Z}_2$ , which is universal by Lagrange theorem. But our choice of  $A, B$  makes  $f$  a 2-anisotropic form ([3]) with a large discriminant  $d(f) = AB$ . By the complete classification of almost universal quaternary quadratic forms ([2]), therefore,  $f$  is not almost universal.

## References

- [1] B. J. Birch, H. Davenport, and D. J. Lewis, The addition of norm forms, *Mathematika* **9** (1962), 75–82.
- [2] J. Bochnak and B.-K. Oh, Almost-universal quadratic forms: An effective solution of a problem of ramanujan, *Duke Math. J.* **147** (2009), no. 1, 131–156.

- [3] J. W. S. Cassels, Rational quadratic forms, London Math. Soc. Monogr. (N.S.), no. 13, 1978.
- [4] H. Davenport, Analytic methods for diophantine equations and diophantine inequalities, 2nd ed., Cambridge University Press, 2005.
- [5] J. Esmonde and M. R. Murty, Problems in algebraic number theory, Grad. Texts in Math., vol. 190, Springer, 2005.
- [6] K. Kato, N. Kurokawa, and T. Saito, Number theory 2: Introduction to class field theory, Translations of mathematical monographs, American Mathematical Soc., 2012.
- [7] P. Ribenboim, Classical theory of algebraic numbers, Springer, 2001.
- [8] R. C. Vaughan, The Hardy-Littlewood method, 2nd ed., Cambridge University Press, 1997.

*Jeongho Park*  
*Department of Mathematics*  
*Postech*  
*San 31 Hyoja Dong, Nam-Gu*  
*Pohang 790-784, Korea*  
*E-mail: pkskng@postech.ac.kr*