STRONG APPROXIMATION AND A CONJECTURE OF HARPAZ AND WITTENBERG

T.D. BROWNING AND D. SCHINDLER

ABSTRACT. We study strong approximation for some algebraic varieties over $\mathbb{Q}$ which are defined using norm forms. This allows us to confirm a special case of a conjecture due to Harpaz and Wittenberg.

CONTENTS

1. INTRODUCTION

This paper establishes a special case of a conjecture due to Harpaz and Wittenberg [HW15, Conj. 9.1], the resolution of which leads to the following very general result about the behaviour of rational points on varieties over $\mathbb{Q}$ admitting a suitable fibration.

Theorem 1.1. *Let X be a smooth proper and geometrically irreducible variety over $\mathbb{Q}$, and let $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a dominant morphism with rationally connected geometric generic fibre. Suppose that $\mathrm{rank}(f) \leqslant 3$, with at least one non-split fibre lying over a rational point of $\mathbb{P}^1_{\mathbb{Q}}$. Assume that there exists a Hilbert subset $H \subset \mathbb{P}^1_{\mathbb{Q}}$ such that $X_c(\mathbb{Q})$ is dense in $X_c(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}(X_c)}$ for every rational point c in H. Then $X(\mathbb{Q})$ is dense in $X(\mathbf{A}_{\mathbb{Q}})^{\mathrm{Br}(X)}$.*

Recall here that the rank of a fibration $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ is defined to be the sum of the degrees of the closed points of $\mathbb{P}^1_{\mathbb{Q}}$ above which the fibre of f is not split. The definition of split fibres can be found in work of Skorobogatov [Sko96], which is where the notion was originally introduced to the subject. The conclusion of Theorem 1.1 is also true when $\operatorname{rank}(f) \leqslant 2$ over any number field, without any condition on the non-split fibres (see [HW15, Thm. 9.31] and its footnote). The latter is due to Harari [Har97] when $\operatorname{rank}(f) = 1$. When $\operatorname{rank}(f) = 2$ and the fibres satisfy weak approximation it follows from work of Colliot-Thélène and Skorobogatov [CTS00]. Thanks to Matthiesen [Mat15] and the work Harpaz and Wittenberg [HW15, Thm. 9.28], the result is also known to be true for arbitrary values of $\operatorname{rank}(f)$ over $\mathbb{Q}$, provided that all the non-split fibres lie over rational points of $\mathbb{P}^1_{\mathbb{Q}}$.

Next, let $K/\mathbb{Q}$ be a finite extension of number fields of degree $n \geqslant 2$ and fix a $\mathbb{Q}$-basis $\{\omega_1, \ldots, \omega_n\}$ for K over $\mathbb{Q}$. For any subfield $F \subset K$, we denote by

$$\mathbf{N}_{K/F}(x_1, \ldots, x_n) = N_{K/F}(x_1\omega_1 + \cdots + x_n\omega_n)$$

the corresponding norm form, where $N_{K/F}$ is the field norm. It follows from work of Derenthal, Smeets and Wei [DSW15, Thm. 2] that the Brauer–Manin obstruction to the Hasse principle or weak approximation is the only obstruction on any smooth proper model X of the affine variety

$$P(t) = \mathbf{N}_{K/\mathbb{Q}}(x_1, \ldots, x_n), \tag{1.1}$$

where $P(t)$ is an irreducible quadratic polynomial over $\mathbb{Q}$. The obvious morphism $X \to \mathbb{P}^1_{\mathbb{Q}}$ has rational geometric generic fibre. It has precisely two non-split fibres over $\mathbb{P}^1_{\mathbb{Q}}$, one of which is the fibre at infinity and the other lies above the quadratic point defined by $P(t)$. Moreover the smooth fibres over $\mathbb{P}^1_{\mathbb{Q}}(\mathbb{Q})$ all satisfy the property that the Brauer–Manin obstruction is the only obstruction to the Hasse principle or weak approximation by work of Sansuc [San81]. Hence Theorem 1.1 applies to X and may be viewed as a considerable generalisation of [DSW15, Thm. 2]. For example, it evidently applies to smooth proper models of the affine varieties in which the right hand side of (1.1) is replaced by a product of norm forms.

Theorem 1.1 will follow from the study of strong approximation for a particular family of varieties defined using norm forms. For any algebraic variety Y defined over $\mathbb{Q}$, we say that strong approximation holds for Y off a finite set S of places of $\mathbb{Q}$ if the image of $Y(\mathbb{Q})$ is dense in the space $Y(\mathbf{A}_{\mathbb{Q}}^S)$ of adèlic points outside S. We will follow the convention that strong approximation off S holds whenever Y fails to have local points at the places of S. Studying strong approximation and the integral Hasse principle on integral models of affine varieties is generally harder than studying weak approximation and the Hasse principle for rational points on proper models of Y.

It is now time to introduce the auxiliary variety W whose arithmetic lies at the heart of Theorem 1.1. For $i \in \{1, 2\}$, let $K_i/\mathbb{Q}$ be an arbitrary number field of degree n_i. Let $L = \mathbb{Q}(\sqrt{a})$ for any $a \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$. We henceforth assume that $L \subset K_1$. In particular n_1 is even. Let $\delta \in L^*$ and let $V \subset \mathbb{A}_{\mathbb{Q}}^{n_1+n_2}$ be the variety given by the equation

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\delta \, \mathbf{N}_{K_1/L}(\mathbf{y})\right) = 2 \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}). \tag{1.2}$$

Let $Z \subset V$ be the codimension two subvariety in which either $\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{y}) = \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}) = 0$ or, if one factors $\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{y})$ (resp. $\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w})$) over $\overline{\mathbb{Q}}$ as a product of linear forms, then two or more of the factors vanish at $\mathbf{y}$ (resp. at $\mathbf{w}$). The auxiliary variety in which we are interested is defined to be the open subset $W = V \setminus Z$. We shall prove the following result.

Theorem 1.2. *Strong approximation holds for W off any non-empty finite set of places.*

Consider momentarily the special case $K_1 = K_2$. Then the variety V in (1.2) first arose in work of Browning and Heath-Brown [BHB12] in their pioneering investigation of the Hasse principle and weak approximation for (1.1). Our variety W is a smooth open subset of V and it contains the variety [BHB12, Eq. (1.8)] as a dense open subset. In particular it follows from [BHB12, Thm. 2] that W satisfies the Hasse principle and weak approximation when $K_1 = K_2$. Although our strategy to prove Theorem 1.2 is inspired by the work of Browning and Heath-Brown [BHB12], it involves a number of new difficulties and ideas on the analytic side. While there is little difficulty in handling $K_1 \neq K_2$ in (1.2), one serious obstacle arises from an extra "square-freeness" condition that occurs when dealing with strong approximation for the particular open set $W \subset V$. In a different direction one is faced with the additional challenge of a sum defining the singular series that is not a priori absolutely convergent. The process of completing and then interpreting the singular series is only achieved through a delicate analysis of local counting functions.

The deduction of Theorem 1.1 from Theorem 1.2 is carried out in §2. The remaining sections are concerned with the proof of Theorem 1.2, beginning with §3, where we relate the statement of the theorem to a suitable counting problem. In §4 we lay down the necessary tools to handle the square-freeness condition that occurs in our work, and for which we build on the work of Matthiesen [Mat15] mentioned above. Finally, in §6 and §7 the main term of our counting function is analysed and shown to satisfy the properties required for the conclusion of Theorem 1.2.

2. Theorem 1.2 implies Theorem 1.1

Our starting point is the construction of W outlined at the start of [HW15, §9.2.2], with data $n = 2$, $k = k_1 = \mathbb{Q}$ and k_2 a quadratic extension of $\mathbb{Q}$. On carrying out a non-singular linear change of variables on (λ, μ), one may clearly assume that $a_1 = 0$ and that a_2 is the square root of a rational number. In this way we arrive at (1.2) with $\delta = b_1 b_2^{-1}$. But then it is straightforward to confirm that the following result is a direct consequence of Theorem 1.2 and [HW15, Cor. 9.10].

Corollary 2.1. *Conjecture 9.1 in* [HW15] *holds when* $n = 2$, $k = k_1 = \mathbb{Q}$ *and* k_2 *is a quadratic extension of* $\mathbb{Q}$.

We may now prove Theorem 1.1. Let $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ be as in the statement of the theorem. In particular the hypotheses (1), (2) and (4) of [HW15, Cor. 9.23] are met (cf. the proof of [HW15, Cor. 9.25]). After a change of coordinates we may assume that the fibre $f^{-1}(\infty)$ is split. Let $M \subset \mathbb{A}^1_{\mathbb{Q}}$ be the finite closed subset containing the points that have a non-split fibre. Then the hypotheses of Theorem 1.1 imply that M contains at least one rational point. If all of the points of M are rational then the result is a special case of a theorem of Matthiesen [Mat15], as recorded in [HW15, Thm. 9.28]. Alternatively, we may suppose that M consists of a rational point and a point defined over a quadratic extension of $\mathbb{Q}$. In this case the statement of Theorem 1.1 is found to be a straightforward consequence of Corollary 2.1 and [HW15, Cor. 9.24].

3. From strong approximation to counting

Let $W \subset \mathbb{A}^{n_1+n_2}_{\mathbb{Q}}$ be the open subset of the variety V in (1.2), as defined in the introduction. According to [CTX13, Prop. 2.2], in order to prove Theorem 1.2 it will suffice to show that the variety W satisfies strong approximation off an arbitrary place v_0 of $\mathbb{Q}$. Let Ω denote the set of places of $\mathbb{Q}$ and write $\mathbf{x} = (\mathbf{y}, \mathbf{w})$ for the vector of variables appearing in the definition of W. We fix an integral model $\mathscr{V}$ for V, which is obtained by clearing denominators from (1.2). This leads to an equation

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\delta \, \mathbf{N}_{K_1/L}(\mathbf{y})\right) = c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}), \tag{3.1}$$

with $a \in \mathbb{Z}$ square-free, $\delta \in \mathfrak{o}_L \backslash \{0\}$ and $c \in 2\mathbb{Z} \backslash \{0\}$. Moreover, we may assume that for $i \in \{1, 2\}$ the norm forms are defined using a $\mathbb{Z}$-basis $\{\omega_1^{(i)}, \dots, \omega_{n_i}^{(i)}\}$ for $\mathfrak{o}_{K_i}$, with $\omega_1^{(i)} = 1$. We let $\mathscr{Z}$ be the scheme-theoretic closure of Z in $\mathscr{V}$ and put $\mathscr{W} = \mathscr{V} \setminus \mathscr{Z}$.

For strong approximation off v_0 on W we must show the following: for any finite set of places $S \subset \Omega \setminus \{v_0\}$, any $(\mathbf{x}_v) \in W(\mathbf{A}_{\mathbb{Q}})$ with $\mathbf{x}_v \in \mathscr{W}(\mathbb{Z}_v)$ for all $v \notin S \cup \{v_0\}$, there exists a point $\mathbf{x} \in W(\mathbb{Q})$ with $\mathbf{x} \in \mathscr{W}(\mathbb{Z}_v)$ for all $v \notin S \cup \{v_0\}$, such that $\mathbf{x}$ is arbitrarily close to $\mathbf{x}_v$ for all $v \in S$. Rather than asking that $\mathbf{x} \in \mathscr{W}(\mathbb{Z}_v)$, for all $v \notin S \cup \{v_0\}$, we shall demand that $\mathbf{x} \in \mathscr{W}^\circ(\mathbb{Z}_v)$ for all $v \notin S \cup \{v_0\}$, where $\mathscr{W}^\circ(\mathbb{Z}_v)$ is the set of points $\mathbf{x} = (\mathbf{y}, \mathbf{w}) \in \mathscr{V}(\mathbb{Z}_v)$ such that

$$
\begin{aligned}
\min\{\operatorname{val}_v(\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{y})), \operatorname{val}_v(\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}))\} &= 0, \\
\max\{\operatorname{val}_v(\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{y})), \operatorname{val}_v(\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}))\} &\leqslant 1.
\end{aligned}
\tag{3.2}
$$

This is clearly stronger than is strictly necessary, but as it turns out, it is easier to handle within the confines of our analytic arguments.

Let $S \subset \Omega \setminus \{v_0\}$ be a finite set of places and let $(\mathbf{x}_v) \in W(\mathbf{A}_{\mathbb{Q}})$, with $\mathbf{x}_v \in \mathscr{W}(\mathbb{Z}_v)$ for all $v \notin S \cup \{\infty, v_0\}$. It will be convenient to put $S_f = S \setminus \{\infty\}$ for the set of finite places in S. There are now two cases to consider, depending on whether or not v_0 is a finite place. Suppose first that $v_0 = \infty$. Then $S = S_f$ and we must find $\mathbf{x} \in W(\mathbb{Q})$ with $\mathbf{x} \in \mathscr{W}^\circ(\mathbb{Z}_v)$, for all $v \notin S_f \cup \{\infty\}$, such that $\mathbf{x}$ is arbitrarily close to $\mathbf{x}_v$ for all $v \in S_f$. Alternatively, suppose that v_0 is a finite place. Without loss of generality we may assume that S contains the infinite place and we put $S_f = S \setminus \{\infty\}$ as before. In this case we must find $\mathbf{x} \in W(\mathbb{Q})$ with $\mathbf{x} \in \mathscr{W}^\circ(\mathbb{Z}_v)$, for all $v \notin S \cup \{v_0\}$, such that $\mathbf{x}$ is arbitrarily close to $\mathbf{x}_v$, for all $v \in S = S_f \cup \{\infty\}$. Thus, when $v_0 = \infty$ we only have to approximate at a finite collection of finite local places S_f, but when v_0 is finite we also have to approximate at the real place.

Let $C \in \mathbb{Z}$ with $C^{-1} \in \mathbb{Z}_{S_f}$ (i.e. all prime factors of C lie in S_f) be chosen so that $\mathbf{x}'_v = (C^{2n_2}\mathbf{y}_v, C^{n_1}\mathbf{w}_v) \in \mathbb{Z}_v^{n_1+n_2}$ for all $v \in S_f$. The change of variables that replaces $\mathbf{x} = (\mathbf{y}, \mathbf{w})$ by $(C^{2n_2}\mathbf{y}, C^{n_1}\mathbf{w})$ clearly maps $(\mathbf{x}_v) \in W(\mathbf{A}_{\mathbb{Q}})$ to $(\mathbf{x}'_v) \in W(\mathbf{A}_{\mathbb{Q}})$, with $\mathbf{x}'_v \in \mathscr{W}(\mathbb{Z}_v)$ for all $v \in \Omega \setminus \{v_0, \infty\}$. By the Chinese remainder theorem we can find $\mathbf{x}^{(M)} \in \mathbb{Z}^{n_1+n_2}$ arbitrarily close to $\mathbf{x}'_v$ for all $v \in S_f$. We now seek a point $\mathbf{x}' = (\mathbf{y}', \mathbf{w}') \in W(\mathbb{Q}) \cap \mathscr{V}(\mathbb{Z})$ which is very close to $\mathbf{x}^{(M)}$ in the v-adic topology for all $v \in S_f$. We further require that $\mathbf{x}' \in \mathscr{W}^\circ(\mathbb{Z}_v)$ for all $v \notin S \cup \{\infty, v_0\}$. The first condition translates into the conditions

$$
\mathbf{y}' \equiv \mathbf{y}^{(M)} \bmod M, \quad \mathbf{w}' \equiv \mathbf{w}^{(M)} \bmod M,
$$

for a suitable positive integer M built from the primes in S_f. The second condition (3.2) can be written

$$
\mu_S^2\left(\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{y}')\,\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}')\right) = 1,
$$

where for any integer k we set

$$\mu_S^2(k) := \begin{cases} 1 & \text{if } p^2 \nmid k \text{ for all primes } p \notin S \cup \{v_0\}, \\ 0 & \text{otherwise.} \end{cases} \qquad (3.3)$$

Once we've found such a vector $\mathbf{x}'$, then this is also very close to $\mathbf{x}_v' \in \mathcal{V}(\mathbb{Z}_v)$ for all $v \in S_f$, and then

$$\mathbf{x} = (C^{-2n_2}\mathbf{y}', C^{-n_1}\mathbf{w}') \in W(\mathbb{Q}) \cap \mathcal{W}(\mathbb{Z}_{S_f \cup \{v_0\}})$$

is very close to $\mathbf{x}_v$ for all $v \in S_f$, with $\mathbf{x} \in \mathcal{W}^\circ(\mathbb{Z}_v)$ for all $v \notin S \cup \{v_0\}$. This will completely answer strong approximation off the infinite place. Let $\varepsilon > 0$ be arbitrary. Whether or not v_0 is a finite place, we will further demand that our rational point $\mathbf{x}' \in W(\mathbb{Q}) \cap \mathcal{V}(\mathbb{Z})$ satisfies

$$|\mathbf{y}'/Y - \mathbf{y}_\infty| < \varepsilon, \quad |\mathbf{w}'/W - \mathbf{w}_\infty| < \varepsilon,$$

for suitable parameters $Y, W > 0$. Define

$$P(k) := \{k^j : j \geqslant 0\}$$

for the set of powers of a positive integer k. If v_0 is a finite place and p_0 is the prime corresponding to v_0 then we will take $Y, W \in P(p_0^{\varphi(M)})$ such that $Y^{n_1} = W^{2n_2}$. Then it is clear that $\mathbf{x}'' = (\mathbf{y}'/Y, \mathbf{w}'/W)$ will satisfy the constraints required to deduce strong approximation off v_0. If $v_0 = \infty$ then the vector $\mathbf{x}'$ is sufficient to deduce strong approximation off infinity and we may allow Y, W to be arbitrary positive real numbers such that $Y^{n_1} = W^{2n_2}$.

To summarise our argument so far, let v_0 be a fixed place of $\mathbb{Q}$ and let $S \subset \Omega \setminus \{v_0\}$ be a finite set of places. There is no loss of generality in assuming that $S \cup \{v_0\}$ contains the primes dividing $acN_{L/\mathbb{Q}}(\delta)$, together with the primes which ramify in K_1 or K_2. We may now draw the following conclusion.

Lemma 3.1. *Assume that* $(\mathbf{x}_v) \in W(\mathbf{A}_\mathbb{Q})$ *Then there exists* $M \in \mathbb{N}$ *and a solution* $(\mathbf{y}^{(M)}, \mathbf{w}^{(M)})$ *of* (3.1) *over* $\mathbb{Z}/M\mathbb{Z}$, *with* $(\mathbf{y}^{(M)}, \mathbf{w}^{(M)}) \equiv (\mathbf{y}_p, \mathbf{w}_p)$ *mod* M *for any prime* $p \in S_f$, *together with a point* $(\mathbf{y}^{(\mathbb{R})}, \mathbf{w}^{(\mathbb{R})}) \in W(\mathbb{R})$, *having the following property. For any* $\varepsilon > 0$ *and all large enough values of* $W, Y \in \mathbb{N}$ *such that* $Y^{n_1} = W^{2n_2}$, *suppose there is a point* $(\mathbf{y}, \mathbf{w}) \in \mathcal{V}(\mathbb{Z})$ *satisfying*

$$\mu_S^2 \left(\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{y}) \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}) \right) = 1,$$

$$\mathbf{y} \equiv \mathbf{y}^{(M)} \bmod M, \quad \mathbf{w} \equiv \mathbf{w}^{(M)} \bmod M,$$

and

$$|\mathbf{y} - Y\mathbf{y}^{(\mathbb{R})}| < \varepsilon Y, \quad |\mathbf{w} - W\mathbf{w}^{(\mathbb{R})}| < \varepsilon W. \qquad (3.4)$$

Then there exists a point $\mathbf{x} \in W(\mathbb{Q})$ *with* $\mathbf{x} \in \mathcal{W}(\mathbb{Z}_v)$ *for all* $v \notin S \cup \{v_0\}$, *such that* $\mathbf{x}$ *is arbitrarily close to* $\mathbf{x}_v$ *for all* $v \in S$.

This result shows that in order to prove that W satisfies strong approximation off v_0 it suffices find $(\mathbf{y}, \mathbf{w}) \in \mathscr{V}(\mathbb{Z})$ satisfying the constraints of the lemma.

Since $(\mathbf{y}^{(\mathbb{R})}, \mathbf{w}^{(\mathbb{R})}) \in W(\mathbb{R})$ we must have $\nabla \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{y}^{(\mathbb{R})}) \neq \mathbf{0}$. In particular $\mathbf{y}^{(\mathbb{R})} \neq \mathbf{0}$. For technical reasons it will be convenient to move $\mathbf{w}^{(\mathbb{R})}$ in (3.1) very slightly, and make a corresponding adjustment in $\mathbf{y}^{(\mathbb{R})}$ to compensate, in order to ensure that we also have $\mathbf{w}^{(\mathbb{R})} \neq \mathbf{0}$. In particular, on choosing ε sufficiently small, we can make sure that that $(\mathbf{y}, \mathbf{w}) \neq (\mathbf{0}, \mathbf{0})$ when (3.4) holds.

We introduce additional bilinear structure by working with a variety of higher dimension. We'll proceed by searching for suitably localised solutions

$$(\mathbf{u}, \mathbf{v}, \mathbf{w}) \in \mathbb{Z}^{n_1} \times \mathbb{Z}^{n_1} \times \mathbb{Z}^{n_2}$$

to the Diophantine equation

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\delta \, \mathbf{N}_{K_1/L}(\mathbf{u}) \, \mathbf{N}_{K_1/L}(\mathbf{v})\right) = c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}). \tag{3.5}$$

Let

$$\mathbf{u}^{(M)} = \mathbf{y}^{(M)}, \quad \mathbf{u}^{(\infty)} = \mathbf{y}^{(\mathbb{R})} \quad \text{and} \quad \mathbf{v}^{(M)} = \mathbf{v}^{(\mathbb{R})} = (1, 0, \ldots, 0).$$

Let $W, U, V \in P(p_0^{\varphi(M)})$ such that $(UV)^{n_1} = W^{2n_2}$. We suppose that we have a solution $(\mathbf{u}, \mathbf{v}, \mathbf{w}) \in \mathbb{Z}^{2n_1 + n_2}$ of (3.5) which satisfies

$$\mu_S^2\left(\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{u}) \, \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{v}) \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w})\right) = 1 \tag{3.6}$$

and

$$\mathbf{u} \equiv \mathbf{u}^{(M)} \bmod M, \quad \mathbf{v} \equiv \mathbf{v}^{(M)} \bmod M, \quad \mathbf{w} \equiv \mathbf{w}^{(M)} \bmod M,$$

and

$$|\mathbf{u} - U\mathbf{u}^{(\mathbb{R})}| < \varepsilon U, \quad |\mathbf{v} - V\mathbf{v}^{(\mathbb{R})}| < \varepsilon V, \quad |\mathbf{w} - W\mathbf{w}^{(\mathbb{R})}| < \varepsilon W.$$

Then if $\mathbf{y} \in \mathbb{Z}^{n_1}$ is the vector corresponding to $(\sum_i u_i \omega_i^{(1)})(\sum_i v_i \omega_i^{(1)})$, when multiplied out and expressed in terms of the integral basis, it is easy to check that the vector $(\mathbf{y}, \mathbf{w}) \in \mathbb{Z}^{n_1 + n_2}$ will be a solution of (3.1) satisfying the conditions of Lemma 3.1 with $Y = UV$.

We employ the notation of "skew-trace" that was introduced in [BHB12]. Thus, if σ is the non-trivial automorphism of L and $\{1, \tau\}$ is a $\mathbb{Z}$-basis for $\mathfrak{o}_L$, we put $\widetilde{\mathrm{Tr}}(x, y) := \mathrm{Tr}_{L/\mathbb{Q}}(x y^\sigma D_L^{-1})$, for $x, y \in L$, where $D_L := \tau - \tau^\sigma$. On writing $x = \delta \, \mathbf{N}_{K_1/L}(\mathbf{u})$ and $y = \left(\mathbf{N}_{K_1/L}(\mathbf{v}) D_L\right)^\sigma$ our equation (3.5) becomes

$$\widetilde{\mathrm{Tr}}(x, y) = c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}),$$

whereas (3.6) becomes $\mu_S^2(N_{L/\mathbb{Q}}(xy)\widetilde{\mathrm{Tr}}(x, y)) = 1$, since S contains all of the places which divide $cN_{L/\mathbb{Q}}(\delta)$ or which ramify in L.

Next, for $i = 1, 2$, we let $\mathfrak{F}^{(i)}$ be a fundamental domain of $\mathfrak{o}_{K_i}/U^+_{K_i}$, where $U^+_{K_i}$ is the group of units of $\mathfrak{o}_{K_i}$ of norm one. It will be convenient to set

$$\mathfrak{F}^{(i)}_X := \{v \in \mathfrak{F}^{(i)} : |N_{K_i/\mathbb{Q}}(v)| \leqslant X\}, \tag{3.7}$$

for any $X \geqslant 1$. We will abuse notation and write $\mathbf{u} \in \mathfrak{F}^{(i)}$ to mean that the point $u_1\omega_1^{(i)} + \cdots + u_{n_i}\omega_{n_i}^{(i)}$ belongs to the region $\mathfrak{F}^{(i)}$. Note that any vector $\mathbf{x} \in \mathbb{R}^{n_i} \cap \mathfrak{F}^{(i)}$ such that $|\mathbf{x}| \leqslant X$ automatically belongs to $\mathfrak{F}^{(i)}_{cX^{n_i}}$ for an appropriate constant $c > 0$ depending only on K_i.

We are now ready to specify the sets over which we will sum. Let G be a further parameter, tending to infinity with V. We then define the regions

$$\mathscr{U} := \left\{\mathbf{u} \in \mathbb{R}^{n_1} \cap \mathfrak{F}^{(1)} : |\mathbf{u} - U\mathbf{u}^{(\mathbb{R})}| < G^{-1}U\right\},$$

$$\mathscr{V} := \left\{\mathbf{v} \in \mathbb{R}^{n_1} \cap \mathfrak{F}^{(1)} : |\mathbf{v} - V\mathbf{v}^{(\mathbb{R})}| < G^{-1}V\right\},$$

$$\mathscr{W} := \left\{\mathbf{w} \in \mathbb{R}^{n_2} \cap \mathfrak{F}^{(2)} : |\mathbf{w} - W\mathbf{w}^{(\mathbb{R})}| < G^{-1}W\right\},$$

where we recall that $(UV)^{n_1} = W^{2n_2}$. In truth the definition of $\mathscr{U}$ should involve a constraint of the form $\max_{1 \leqslant i \leqslant n_1} |L_i(\mathbf{u}) - UL_i(\mathbf{u}^{(\mathbb{R})})| < G^{-1}U$ for suitable independent linear forms $L_1, \ldots, L_{n_1}$ (cf. [BHB12, Eq. (3.14)]) that are constructed for the sole purpose of proving [BHB12, Lemma 9]. Since we will later use the latter result as a "black box", we have decided to ease notation by working under the assumption that $L_i(\mathbf{u}) = u_i$ for $1 \leqslant i \leqslant n_1$.

For technical convenience we introduce an additional restriction on the values of $\mathbf{v}$ that we consider. If we write $N_{K_1/L}(\mathbf{v}) = N_1(\mathbf{v}) + N_2(\mathbf{v})\tau$, then we impose the condition that

$$\gcd(N_1(\mathbf{v}), N_2(\mathbf{v})) = 1. \tag{3.8}$$

Let

$$\alpha(x) := \#\left\{\mathbf{u} \in \mathscr{U} \cap \mathbb{Z}^{n_1} : \ \mathbf{u} \equiv \mathbf{u}^{(M)} \bmod M, \ \delta \, \mathbf{N}_{K_1/L}(\mathbf{u}) = x \right\}, \tag{3.9}$$

$$\beta(y) := \#\left\{\mathbf{v} \in \mathscr{V} \cap \mathbb{Z}^{n_1} : \begin{array}{l} \mathbf{v} \equiv \mathbf{v}^{(M)} \bmod M, \ (3.8) \text{ holds} \\ (\mathbf{N}_{K_1/L}(\mathbf{v})D_L)^\sigma = y \end{array} \right\}, \tag{3.10}$$

for $x, y \in \mathfrak{o}_L$. Lastly, we define the function

$$\lambda(l) := \#\left\{\mathbf{w} \in \mathscr{W} \cap \mathbb{Z}^{n_2} : \mathbf{w} \equiv \mathbf{w}^{(M)} \bmod M, \ c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}) = l\right\}, \tag{3.11}$$

for $l \in \mathbb{Z}$. Notice that $\mathbf{u}^{(\mathbb{R})}, \mathbf{v}^{(\mathbb{R})}, \mathbf{w}^{(\mathbb{R})}$ are all non-zero, whence $\mathbf{u}, \mathbf{v}, \mathbf{w}$ will be non-zero throughout $\mathscr{U}, \mathscr{V}$ and $\mathscr{W}$, if G is large enough. It follows in particular that α, β are supported on non-zero $x, y \in \mathfrak{o}_L$ and λ is supported on non-zero integers.

We proceed to define the bilinear form

$$\mathscr{N}(G, U, V, W) := \sum_{x,y \in \mathfrak{o}_L} \mu_S^2 \left(N_{L/\mathbb{Q}}(xy) \widetilde{\mathrm{Tr}}(x, y) \right) \alpha(x) \beta(y) \lambda \big(\widetilde{\mathrm{Tr}}(x, y) \big). \quad (3.12)$$

Our argument thus far shows that Theorem 1.2 holds if we can show that $\mathscr{N}(G, U, V, W) > 0$ for all sufficiently large values of $G, U, V, W > 0$ such that $(UV)^{n_1} = W^{2n_2}$. In order to handle the square-freeness condition, we put

$$Sv_0 = \begin{cases} p_0 \prod_{p \in S_f} p & \text{if } v_0 \neq \infty, \\ \prod_{p \in S_f} p & \text{if } v_0 = \infty, \end{cases} \quad (3.13)$$

where p_0 is the prime corresponding to v_0 when it is finite. We may now rewrite (3.3) as

$$\mu_S^2(k) = \sum_{\substack{d^2 \mid k \\ (d, Sv_0) = 1}} \mu(d), \quad (3.14)$$

which allows us to trade the square-freeness condition for congruence conditions. For small values of d it is possible to adapt the argument in [BHB12] satisfactorily. The necessary tools for handling the contribution from large values of d are laid out in the next section.

4. Handling square-freeness

4.1. **Technical tools.** We begin with an estimate for the mean square of the functions defined in (3.9)–(3.11). The proof of [BHB12, Lemma 4] easily gives the following estimates.

Lemma 4.1. *Let $x \in \mathfrak{o}_L$ and $l \in \mathbb{Z}$ be given. Then for any $\eta > 0$ we have $\alpha(x) \ll_\eta U^\eta$, $\beta(x) \ll_\eta V^\eta$ and $\lambda(l) \ll_\eta W^\eta$.*

It will be convenient to record the mean square estimates

$$\sum_{x \in \mathfrak{o}_L} |\alpha(x)|^2 \ll_\eta U^{n_1 + \eta}, \quad \sum_{y \in \mathfrak{o}_L} |\beta(y)|^2 \ll_\eta V^{n_1 + \eta}, \quad \sum_{l \in \mathbb{Z}} |\lambda(l)|^2 \ll_\eta W^{n_2 + \eta},$$

which are easy consequences of Lemma 4.1.

Let $K/\mathbb{Q}$ be a number field of degree n. Let $d \in \mathbb{N}$ be square-free and let $\mathfrak{F}_X$ be as in (3.7), where $\mathfrak{F}$ is a fundamental domain of $\mathfrak{o}_K / U_K^+$. We put $\mathscr{R}(X) := \mathbb{Z}^n \cap \mathfrak{F}_X$ for ease of notation, and proceed to define the counting functions

$$M_d(X) := \# \left\{ \mathbf{x} \in \mathscr{R}(X) : d^2 \mid \mathbf{N}_{K/\mathbb{Q}}(\mathbf{x}) \right\},$$
$$N_d(\boldsymbol{X}) := \# \left\{ (\mathbf{x}, \mathbf{y}) \in \mathscr{R}(X_1) \times \mathscr{R}(X_2) : d \mid \big(\mathbf{N}_{K/\mathbb{Q}}(\mathbf{x}), \mathbf{N}_{K/\mathbb{Q}}(\mathbf{y}) \big) \right\}, \quad (4.1)$$

for any $d \in \mathbb{N}$ and $X \in \mathbb{R}_{>0}$ and $\boldsymbol{X} = (X_1, X_2) \in \mathbb{R}_{>0}^2$. By adapting an argument of Matthiesen [Mat15, Lemma 3.1] we will show that $M_d(X)$ and

$N_d(\boldsymbol{X})$ are both small for large square-free values of d. This is the purpose of the following result, which is absolutely pivotal in our work.

Lemma 4.2. *Let $\varepsilon > 0$ and let $d \in \mathbb{N}$ be square-free. Then*

$$M_d(X) \ll_\varepsilon \frac{X}{d^{2-\varepsilon}} \quad and \quad N_d(\boldsymbol{X}) \ll_\varepsilon \frac{X_1 X_2}{d^{2-\varepsilon}},$$

where the implied constants depend at most on K and the choice of ε.

Proof. Put $R(m) := \#\{\mathbf{x} \in \mathbb{Z}^n \cap \mathfrak{F} : \mathbf{N}_{K/\mathbb{Q}}(\mathbf{x}) = m\}$, for any integer m. It follows from [BM15, Lemma 8.1] that $R(m) \ll r_K(|m|)$, where r_K is the multiplicative arithmetic function that appears as coefficients of the Dedekind zeta function $\zeta_K(s)$.

It follows that

$$M_d(X) = \sum_{\substack{|m| \leqslant X \\ d^2 | m}} R(m) \ll \sum_{\substack{m \leqslant X \\ d^2 | m}} r_K(m) = \sum_{m \leqslant X/d^2} r_K(d^2 m).$$

Let us factorise $m = hm'$, where $h \mid d^\infty$ and m' is coprime d. Then we have $r_K(d^2 m) = r_K(d^2 h) r_K(m')$ by multiplicativity. Hence

$$M_d(X) \ll \sum_{h | d^\infty} r_K(d^2 h) \sum_{m' \leqslant X/(d^2 h)} r_K(m').$$

The inner sum is $O(X/(d^2 h))$ by [BM15, Eq. (2.8)]. Furthermore, for any $\varepsilon > 0$, we have $r_K(d^2 h) \leqslant \tau(d^2 h) \ll_\varepsilon (dh)^{\varepsilon/2}$ by [BM15, Eq. (2.10)]. Hence it follows that

$$M_d(X) \ll_\varepsilon X \sum_{h | d^\infty} \frac{(dh)^{\varepsilon/2}}{d^2 h} \ll_\varepsilon \frac{X}{d^{2-\varepsilon}},$$

as required, since

$$\sum_{h | d^\infty} \frac{h^{\varepsilon/2}}{h} \leqslant \sum_{h | d^\infty} \frac{1}{\sqrt{h}} = \prod_{p | d} \left(1 - \frac{1}{\sqrt{p}}\right)^{-1} \ll_\varepsilon d^{\varepsilon/2}.$$

In a similar fashion we find that

$$N_d(\boldsymbol{X}) = \sum_{\substack{|m_1| \leqslant X_1 \\ d | m_1}} R(m_1) \sum_{\substack{|m_2| \leqslant X_2 \\ d | m_2}} R(m_2)$$

$$\ll \sum_{h_1, h_2 | d^\infty} r_K(dh_1) r_K(dh_2) \prod_{i=1,2} \sum_{m_i' \leqslant X_i/(dh_i)} r_K(m_i')$$

$$\ll_\varepsilon \frac{X_1 X_2}{d^{2-\varepsilon}}.$$

This completes the proof of the lemma. $\square$

4.2. **Reduction to small moduli.** Armed with Lemma 4.2, we now return to our analysis of $\mathcal{N}(G, U, V, W)$, as defined in (3.12), with the aim of handling the constraint $\mu_S^2(N_{L/\mathbb{Q}}(xy)\widetilde{\mathrm{Tr}}(x, y)) = 1$. We will henceforth take

$$U = H^{n_2}V_0^{n_2}, \quad V = V_0^{n_2}, \quad W = H^{n_1/2}V_0^{n_1}. \tag{4.2}$$

for $V \geqslant H \geqslant 1$. One sees immediately that $(UV)^{n_1} = W^{2n_2}$ with these choices. Note that we will ultimately take $G = \log V$.

We recall the convention regarding the parameters H and V from [BHB12]. H will be taken to be a small fixed power of V. There will be certain points in our argument where additional factors of V^η will appear with arbitrary small $\eta > 0$. This will not matter since we will ultimately make a key saving which is a power of H, so that the error term makes a satisfactory overall contribution. Let us henceforth write $\mathcal{N}(G, U, V, W) = \mathcal{N}(G, H, V)$ to better reflect our choice of U and W. Thus

$$\mathcal{N}(G, H, V) = \sum_{x,y \in \mathfrak{o}_L} \mu_S^2\left(N_{L/\mathbb{Q}}(xy)\widetilde{\mathrm{Tr}}(x, y)\right) \alpha(x)\beta(y)\lambda\left(\widetilde{\mathrm{Tr}}(x, y)\right).$$

In view of (3.9), we see that the function α is supported on $x_1 + \tau x_2 \in \mathfrak{o}_L$ such that $x_1, x_2 \ll U^{n_1/2}$. Similarly, (3.10) and (3.11) show that β (resp. λ) is supported on $y_1 + \tau y_2 \in \mathfrak{o}_L$ such that $y_1, y_2 \ll V^{n_1/2}$ (resp. $l \in \mathbb{Z}$ such that $l \ll W^{n_2}$).

Lemma 4.1 yields $\mathcal{N}(G, H, V) \ll_\eta (UV)^{n_1+\eta}W^\eta \ll_\eta H^{n_1 n_2}V_0^{2n_1 n_2+O(\eta)}$, for any $\eta > 0$. The remainder of this paper is dedicated to proving a commensurate lower bound, as follows.

Theorem 4.3. *Let* $G = \log V$ *and let* $H = V^{\frac{1}{n_1 n_2^2(n_1+16)}}$. *Then we have*

$$\mathcal{N}(G, H, V) \gg (\log V)^{1-2n_1-n_2} H^{n_1 n_2}V_0^{2n_1 n_2}.$$

We begin by simplifying the square-freeness constraint.

Lemma 4.4. *For any* $x, y \in \mathfrak{o}_L$ *we have*

$$\mu_S^2\left(N_{L/\mathbb{Q}}(xy)\widetilde{\mathrm{Tr}}(x, y)\right) = \mu_S^2\left(N_{L/\mathbb{Q}}(xy)\right) \mu_S^2\left(\widetilde{\mathrm{Tr}}(x, y)\right).$$

Proof. We write everything out in terms of the basis $\{1, \tau\}$ for $\mathfrak{o}_L$, so that $x = x_1 + \tau x_2$ and $y = y_1 + \tau y_2$. Thus gives

$$N_{L/\mathbb{Q}}(x) = x_1^2 + x_2^2 N_{L/\mathbb{Q}}\tau + x_1 x_2 \mathrm{Tr}_{L/\mathbb{Q}} \tau,$$
$$N_{L/\mathbb{Q}}(y) = y_1^2 + y_2^2 N_{L/\mathbb{Q}}\tau + y_1 y_2 \mathrm{Tr}_{L/\mathbb{Q}} \tau,$$
$$\widetilde{\mathrm{Tr}}(x, y) = x_2 y_1 - x_1 y_2,$$

since $\mathrm{Tr}_{L/\mathbb{Q}}(1/(\tau - \tau^\sigma)) = 0$ and $\mathrm{Tr}_{L/\mathbb{Q}}(\tau/(\tau - \tau^\sigma)) = 1$. Assuming that $\mu_S^2(N_{L/\mathbb{Q}}(xy)) = 1$, it suffices to show that there is no common prime divisor p

of $\widetilde{\mathrm{Tr}}(x,y)$ and $N_{L/\mathbb{Q}}(x)$ such that $p \nmid Sv_0$. To see this, we suppose otherwise for a contradiction. We may assume that one of y_1 or y_2 is coprime to p, else we would have $p^2 \mid N_{L/\mathbb{Q}}(y)$. Suppose that $p \nmid y_1$ and let $\overline{y_1}$ denote the multiplicative inverse of y_1 modulo p. Then $p \mid \widetilde{\mathrm{Tr}}(x,y)$ implies that $x_2 \equiv x_1 \overline{y}_1 y_2 \bmod p$. Next, we deduce from $p \mid N_{L/\mathbb{Q}}(x)$ that

$$x_1^2 \left(1 + (\overline{y}_1 y_2)^2 N_{L/\mathbb{Q}} \tau + \overline{y}_1 y_2 \operatorname{Tr}_{L/\mathbb{Q}} \tau \right) \equiv 0 \bmod p.$$

But this is equivalent to $p \mid N_{L/\mathbb{Q}}(y)$, since we cannot have $p \mid x_1$, which in turn implies that $p^2 \mid N_{L/\mathbb{Q}}(xy)$. This is a contradiction and so completes the proof of the lemma. $\qquad\square$

Given non-zero integers a, b, let us write $(a,b)_S$ for the greatest common divisor of a and b which is coprime to Sv_0, in the notation of (3.13). Lemma 4.4 implies that

$$\mathscr{N}(G,H,V) = \sum_{\substack{x,y \in \mathfrak{o}_L \\ (N_{L/\mathbb{Q}}(x), N_{L/\mathbb{Q}}(y))_S = 1}} \mu_S^2\left(N_{L/\mathbb{Q}}(x)\right) \mu_S^2\left(N_{L/\mathbb{Q}}(y)\right) \mu_S^2\left(\widetilde{\mathrm{Tr}}(x,y)\right)$$
$$\times \alpha(x)\beta(y)\lambda\big(\widetilde{\mathrm{Tr}}(x,y)\big).$$

We use Möbius inversion to take care of the coprimality condition and (3.14) to open up the factors involving μ_S^2. This leads to the conclusion that

$$\mathscr{N}(G,H,V) = \sum_{\substack{d,e,f,k=1 \\ (defk,Sv_0)=1}}^{\infty} \mu(d)\mu(e)\mu(f)\mu(k) \sum_{\substack{x,y \in \mathfrak{o}_L \\ [d^2,k] \mid N_{L/\mathbb{Q}}(x) \\ [e^2,k] \mid N_{L/\mathbb{Q}}(y) \\ f^2 \mid \widetilde{\mathrm{Tr}}(x,y)}} \alpha(x)\beta(y)\lambda\big(\widetilde{\mathrm{Tr}}(x,y)\big).$$

We separate out the contribution

$$\mathscr{N}_\xi(G,H,V) = \sum_{\substack{d,e,f,k \leqslant V^\xi \\ (defk,Sv_0)=1}} \mu(d)\mu(e)\mu(f)\mu(k)$$
$$\times \sum_{\substack{x,y \in \mathfrak{o}_L \\ [d^2,k] \mid N_{L/\mathbb{Q}}(x) \\ [e^2,k] \mid N_{L/\mathbb{Q}}(y) \\ f^2 \mid \widetilde{\mathrm{Tr}}(x,y)}} \alpha(x)\beta(y)\lambda\big(\widetilde{\mathrm{Tr}}(x,y)\big), \qquad (4.3)$$

from small values of d, e, f, k. The reader should think of ξ as being a fixed but small positive real number. Our next task is to show that

$$\mathscr{N}(G,H,V) = \mathscr{N}_\xi(G,H,V) + O_\eta\left(H^{n_1 n_2} V_0^{2n_1 n_2 - \xi + O(\eta)}\right), \qquad (4.4)$$

for any $\eta > 0$. This means, on taking η sufficiently small in terms of ξ, that in order to prove Theorem 4.3 we may henceforth focus on a lower bound for $\mathscr{N}_\xi(G, H, V)$ for any fixed $\xi > 0$.

To establish the claim let us first consider the overall contribution from $d > V^\xi$. Since α, β, λ are supported away from zero, this means that there are $O_\eta(V^\eta)$ choices for e, f, k for a fixed choice of x, y appearing in the sum, by the standard estimate for the divisor function. Applying Lemma 4.1 to estimate β and λ, we open up α to find that this contribution is

$$\ll_\eta V^{n_1+O(\eta)} \sum_{d>V^\xi} \mu^2(d) \sum_{\substack{x\in\mathfrak{o}_L \\ d^2|N_{L/\mathbb{Q}}(x)}} \alpha(x) \ll_\eta V^{n_1+O(\eta)} \sum_{d>V^\xi} \mu^2(d) M_d(cU^{n_1}),$$

in the notation of (4.1), for an appropriate constant $c > 0$ depending on K_1. But now we invoke Lemma 4.2 to bound this by

$$\ll_\eta V^{n_1+O(\eta)} \sum_{d>V^\xi} \frac{U^{n_1}}{d^{2-\eta}} \ll_\eta (UV)^{n_1} V^{-\xi+O(\eta)},$$

as claimed. The same argument deals with the contribution from e exceeding V^ξ. Similarly, on applying Lemma 4.1 to estimate λ, we open up α and β to find that the contribution from $k > V^\xi$ is

$$\ll_\eta V^{O(\eta)} \sum_{k>V^\xi} \mu^2(k) \sum_{\substack{x,y\in\mathfrak{o}_L \\ k|(N_{L/\mathbb{Q}}(x),N_{L/\mathbb{Q}}(y))}} \alpha(x)\beta(y)$$

$$\ll_\eta V^{O(\eta)} \sum_{k>V^\xi} \mu^2(k) N_k(cU^{n_1}, cV^{n_1}),$$

for an appropriate constant $c > 0$, in the notation of (4.1). Lemma 4.2 therefore shows that this makes an overall contribution $O_\eta((UV)^{n_1}V^{-\xi+O(\eta)})$, as required. Finally, using the same strategy, the contribution from $f > V^\xi$ is seen to be

$$\ll_\eta V^{O(\eta)} \sum_{f>V^\xi} \mu^2(f) \sum_{\substack{\mathbf{w}\in\mathscr{W}\cap\mathbb{Z}^{n_2} \\ f^2|c\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w})}} N(\mathbf{w}),$$

where $N(\mathbf{w})$ denotes the number of $x, y \in \mathfrak{o}_L$ for which $\alpha(x)\beta(y) \neq 0$ and $\widetilde{\mathrm{Tr}}(x,y) = c\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w})$. Writing $x = x_1 + \tau x_2$ and $y = y_1 + \tau y_2$, so that $\widetilde{\mathrm{Tr}}(x,y) = x_2 y_1 - x_1 y_2$, the condition $\alpha(x)\beta(y) \neq 0$ ensures that $x_1, x_2 \ll U^{n_1/2}$ and $y_1, y_2 \ll V^{n_1/2}$. Hence it follows from the standard estimate for the divisor function that $N(\mathbf{w}) = O_\eta(U^{n_1/2}V^{n_1/2+\eta})$. Applying Lemma 4.2 to estimate the

number of $\mathbf{w}$ we obtain the contribution

$$\ll_\eta (UV)^{n_1/2} V^{O(\eta)} \sum_{f>V^\xi} \mu^2(f) \frac{W^{n_2}}{f^{2-\eta}} \ll_\eta (UV)^{n_1} V^{-\xi+O(\eta)},$$

which is also satisfactory. This completes the proof of (4.4).

4.3. **Preliminary analysis of** $\mathscr{N}_\xi(G,H,V)$. In this section we prepare the evaluation of the main term (4.3). We split the contribution according to the residue classes of $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$. In the following we write

$$m = [d^2, e^2, f^2, k].$$

In particular, we have $(m, Sv_0) = 1$ and $m \leqslant V^{7\xi}$. Let $\mathscr{S}(d,e,f,k)$ be the set of residue classes $\mathbf{u}, \mathbf{v} \in (\mathbb{Z}/m\mathbb{Z})^{n_1}$ and $\mathbf{w} \in (\mathbb{Z}/m\mathbb{Z})^{n_2}$ such that

$$[d^2, k] | N_{L/\mathbb{Q}}(\delta \, \mathbf{N}_{K_1/L}(\mathbf{u})), \quad [e^2, k] | N_{L/\mathbb{Q}}(\mathbf{N}_{K_1/L}(\mathbf{v})D_L), \quad f^2 | c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}).$$

Let $(\mathbf{u}^{(m)}, \mathbf{v}^{(m)}, \mathbf{w}^{(m)}) \in \mathscr{S}(d,e,f,k)$. We denote by $\mathbf{u}^{(M,m)} \in (\mathbb{Z}/mM\mathbb{Z})^{n_1}$ the vector which reduces to $\mathbf{u}^{(M)}$ modulo M and to $\mathbf{u}^{(m)}$ modulo m, and similarly for $\mathbf{v}^{(M,m)}, \mathbf{w}^{(M,m)}$. Furthermore, as in §3, we define the counting functions

$$\alpha_{m,\mathbf{u}^{(m)}}(x) := \#\{\mathbf{u} \in \mathscr{U} \cap \mathbb{Z}^{n_1} : \mathbf{u} \equiv \mathbf{u}^{(M,m)} \bmod Mm, \ \delta \, \mathbf{N}_{K_1/L}(\mathbf{u}) = x\},$$

$$\beta_{m,\mathbf{v}^{(m)}}(y) := \#\left\{\mathbf{v} \in \mathscr{V} \cap \mathbb{Z}^{n_1} : \begin{array}{l} \mathbf{v} \equiv \mathbf{v}^{(M,m)} \bmod Mm, \\ (\mathbf{N}_{K_1/L}(\mathbf{v})D_L)^\sigma = y, \ (3.8) \text{ holds} \end{array}\right\},$$

for $x, y \in \mathfrak{o}_L$, and

$$\lambda_{m,\mathbf{w}^{(m)}}(l) := \#\left\{\mathbf{w} \in \mathscr{W} \cap \mathbb{Z}^{n_2} : \mathbf{w} \equiv \mathbf{w}^{(M,m)} \bmod Mm, \ c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}) = l\right\},$$

for $l \in \mathbb{Z}$. Furthermore, we define

$$\mathscr{N}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}} = \sum_{x,y\in\mathfrak{o}_L} \alpha_{m,\mathbf{u}^{(m)}}(x) \beta_{m,\mathbf{v}^{(m)}}(y) \lambda_{m,\mathbf{w}^{(m)}}\big(\widetilde{\mathrm{Tr}}(x,y)\big). \qquad (4.5)$$

The dependence of this function on G, H, V is to be understood implicitly. Then we have

$$\mathscr{N}_\xi(G,H,V) = \sum_{\substack{d,e,f,k \leqslant V^\xi \\ (defk, Sv_0)=1}} \mu(d)\mu(e)\mu(f)\mu(k)$$

$$\times \sum_{(\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)})\in\mathscr{S}(d,e,f,k)} \mathscr{N}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}}. \qquad (4.6)$$

Our next goal is to evaluate $\mathscr{N}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}}$ for fixed m and fixed vectors $\mathbf{u}^{(m)}$, $\mathbf{v}^{(m)}$, and $\mathbf{w}^{(m)}$.

5. Approximating functions

In this section we use results from §4 and §5 from [BHB12] to find an approximation $\widehat{\alpha}_{m,\mathbf{u}^{(m)}}(x)$ to $\alpha_{m,\mathbf{u}^{(m)}}(x)$. The main difference is that in [BHB12] the modulus M was fixed and all implied constants were allowed to depend on it. In our situation $\alpha_{m,\mathbf{u}^{(m)}}(x)$ also depends on m, which varies in our argument. Hence we need to indicate explicitly the dependence on m in all our estimates. As the proofs are almost the same, we omit most of the details.

We start by constructing a function $\omega_m(x)$ such that the conditions [BHB12, Eqs. (4.8)–(4.11)] are satisfied. For this let

$$\omega_m(x) := (Mm)^{-n_1}\omega_1(x), \tag{5.1}$$

where $\omega_1(x)$ is the function constructed and described in [BHB12, Lemma 9], with associated parameters $M = 1$ and $n = n_1$.

Let $\widehat{\alpha}_{m,\mathbf{u}^{(m)}}(x)$ be defined as [BHB12, Eq. (4.13)] with $\omega(x)$ replaced by $\omega_m(x)$, in the notation of (5.1), and with the density function

$$\varrho^{(m)}(y,q) := \frac{(Mm)^{n_1}}{[Mm,q]^{n_1}}\#\left\{\mathbf{s} \bmod [Mm,q] : \begin{array}{l} \mathbf{s} \equiv \mathbf{u}^{(M,m)} \bmod Mm \\ \delta\,\mathbf{N}_{K_1/L}(\mathbf{s}) \equiv y \bmod q \end{array}\right\}.$$

Thus we have

$$\widehat{\alpha}_{m,\mathbf{u}^{(m)}}(x) = \omega_m(x)\sum_{q\leqslant Q}\sideset{}{^*}\sum_{t \bmod q} e_q^{(L)}(-tx)\sum_{z \bmod q}\varrho^{(m)}(z,q)e_q^{(L)}(tz),$$

where the summation $\sum_{t \bmod q}^{*}$ is understood as a summation of $t = t_1 + t_2\tau$ with $t \in \mathbb{Z}/q\mathbb{Z}$ and $(q,t_1,t_2) = 1$, and we recall that $e_q^{(L)}(x) := e_q(b)$ for $x = a + b\tau \in L$ with $a, b \in \mathbb{Q}$ and $q \in \mathbb{N}$.

By rescaling, we see that condition (4.11) in [BHB12] is satisfied for the parameters $W \ll (Mm)^{-n_1}U^{n_1-1}$ and $Q \leqslant U^{1/2}$. Both of the conditions (4.9) and (4.10) in [BHB12] are clear from the definition of the densities $\varrho^{(m)}(y,q)$. Moreover, a short calculation reveals that condition (4.8) in [BHB12] holds with $E \ll_\eta m^{n_1+1}Q^{n_1+1}U^{n_1-1+\eta}$. Let $\alpha_{m,\mathbf{u}^{(m)}}^{\dagger}(x) := \alpha_{m,\mathbf{u}^{(m)}}(x) - \widehat{\alpha}_{m,\mathbf{u}^{(m)}}(x)$. An application of [BHB12, Lemma 7] gives the following lemma.

Lemma 5.1. *Let R be a square in the (x_1, x_2)-plane with sides parallel to the coordinate axes and with side length $\varrho \geqslant 1$ satisfying $\varrho \ll U^{n_1/2}$. Then*

$$\left|\sum_{\substack{x\in R \\ x\equiv y \bmod q}} \alpha_{m,\mathbf{u}^{(m)}}^{\dagger}(x)\right| \ll_\eta m^{n_1+1}Q^{n_1+1}U^{n_1-1+\eta},$$

for any $\eta > 0$, $n_1 \geqslant 3$ and all y modulo q for $q \leqslant Q \leqslant U^{1/2}$.

Moreover, [BHB12, Lemma 8] yields the following L^2-bound for $\widehat{\alpha}_{m,\mathbf{u}^{(m)}}(x)$.

Lemma 5.2. *For any $\eta > 0$ one has*

$$\sum_{x \in \mathfrak{o}_L} |\widehat{\alpha}_{m,\mathbf{u}^{(m)}}(x)|^2 \ll_\eta U^{n_1+\eta} G^{2n_1},$$

for $Q^2 \leqslant U$, $G \leqslant U^{1/(n_1+1)}$ and $Q^{n_1+5}(Mm)^{n_1+1} \leqslant U^{1-\eta}$.

Finally, we observe that

$$\sum_{x \in \mathfrak{o}_L} |\alpha^\dagger_{m,\mathbf{u}^{(m)}}(x)|^2 \ll \sum_{x \in \mathfrak{o}_L} |\alpha_{m,\mathbf{u}^{(m)}}(x)|^2 + \sum_{x \in \mathfrak{o}_L} |\widehat{\alpha}_{m,\mathbf{u}^{(m)}}(x)|^2 \ll_\eta U^{n_1+\eta} G^{2n_1}.$$

Next we apply [BHB12, Lemma 13] to the function $\alpha^\dagger_{m,\mathbf{u}^{(m)}}(x)$. Here one can verify that the parameters $W_0 = m^{n_1+1} Q^{n_1+1} U^{n_1-1+\eta}$ (which is a consequence of Lemma 5.1) and $A_0 \ll_\eta Q^3 U^\eta$ form an admissible choice. We obtain the following result.

Lemma 5.3. *Let $\eta > 0$, $Q \leqslant Q_0 \leqslant U^{1/(n_1+16)}$ and $G \leqslant U^{1/(n_1+1)}$. Then*

$$\sum_{q \leqslant Q_0} q^2 \sum_{y \bmod q} \max_R \left| \sum_{\substack{x \in R \\ x \equiv y \bmod q}} \alpha^\dagger_{m,\mathbf{u}^{(m)}}(x) \right|^2 \ll_\eta Q_0 Q^{-1} (Mm)^{2(n_1+1)} U^{2n_1+6\eta} G^{2n_1}.$$

We now consider the error term

$$\mathscr{E}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}} = \sum_{x,y \in \mathfrak{o}_L} \alpha^\dagger_{m,\mathbf{u}^{(m)}}(x) \beta_{m,\mathbf{v}^{(m)}}(y) \lambda_{m,\mathbf{w}^{(m)}}\big(\widetilde{\mathrm{Tr}}(x,y)\big).$$

As in [BHB12, Lemma 15] the above estimates allow us to provide the following bound on $\mathscr{E}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}}$.

Lemma 5.4. *Let $G = \log V$, let $m \leqslant V^{7\xi}$ and assume that*

$$(\log V)^{16} \ll Q \ll \min\{H^{4n_1n_2/7}, H^{-4n_1n_2} U^{8/(n_1+16)}\}. \tag{5.2}$$

Then

$$\mathscr{E}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}} \ll_\eta Q^{-1/16} m^{(n_1+1)/2} V_0^{2n_1n_2+O(\eta)} H^{n_1n_2}.$$

6. EVALUATION OF THE MAIN TERM

In this section we evaluate the main term contributing to the counting function (4.5), which is given by

$$\mathscr{M}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}} := \sum_{x,y \in \mathfrak{o}_L} \widehat{\alpha}_{m,\mathbf{u}^{(m)}}(x) \beta_{m,\mathbf{v}^{(m)}}(y) \lambda_{m,\mathbf{w}^{(m)}}\big(\widetilde{\mathrm{Tr}}(x,y)\big).$$

At this point we can still closely follow the arguments in [BHB12, §8]. For this we first introduce some notation. We define

$$F(\mathbf{v}, \mathbf{w}, \mathbf{s}) := 2^{-\kappa} \left(\mathrm{Tr}_{L/\mathbb{Q}}(\delta \, \mathbf{N}_{K_1/L}(\mathbf{s}) \, \mathbf{N}_{K_1/L}(\mathbf{v})) - c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}) \right),$$

where $\kappa = 1$ if $2 \mid \mathrm{Tr}_{L/\mathbb{Q}}(\tau)$ and $\kappa = 0$ if $2 \nmid \mathrm{Tr}_{L/\mathbb{Q}}(\tau)$. Moreover, we introduce the notation

$$a_1 = \mathrm{Tr}_{L/\mathbb{Q}}(\mathbf{N}_{K_1/L}(\mathbf{v})), \quad a_2 = \mathrm{Tr}_{L/\mathbb{Q}}(\tau\, \mathbf{N}_{K_1/L}(\mathbf{v})) \quad \text{and} \quad b = c\,\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{w}).$$

In approximating the sums in the main term with integrals one is lead to consider

$$I(\mathbf{v}, \mathbf{w}) := \int_{-\infty}^{\infty} \omega_m(a_2 x, -a_1 x + b/a_2)\mathrm{d}x,$$

if $a_2 \neq 0$. (If $a_2 = 0$ and $a_1 \neq 0$ then it is to be understood that one replaces the integrand by $\omega_m(-a_2 x + b/a_1, a_1 x)$ in this definition.)

At the finite places one is lead to considering the system of congruences

$$(\mathbf{p}, \mathbf{q}, \mathbf{s}) \equiv (\mathbf{v}^{(M,m)}, \mathbf{w}^{(M,m)}, \mathbf{u}^{(M,m)}) \bmod Mm, \tag{6.1}$$

and

$$F(\mathbf{p}, \mathbf{q}, \mathbf{s}) \equiv 0 \bmod u, \quad \text{and} \quad l \mid \mathbf{N}_{K_1/L}(\mathbf{p}). \tag{6.2}$$

We write $\Delta = [Mm, u, l]$. For given positive integers l, u, we define the counting function $N_{M,m}(l, u)$ to be the number of tuples $(\mathbf{p}, \mathbf{q}, \mathbf{s})$ modulo Δ such that (6.1) and (6.2) hold.

We now define the truncated singular series

$$\tilde{\mathfrak{S}}^{(m)}(Q) := \sum_{q \leqslant Q} \sum_{l=1}^{\infty} \mu(l) \sum_{u \mid q} \frac{u\mu(q/u)}{\Delta^{2n_1+n_2}} N_{M,m}(l, u)$$

and the singular integral

$$\sigma_\infty := m^{n_1} \sum_{\mathbf{w} \in \mathscr{W} \cap \mathbb{Z}^{n_2}} \sum_{\mathbf{v} \in \mathscr{V} \cap \mathbb{Z}^{n_1}} I(\mathbf{v}, \mathbf{w}). \tag{6.3}$$

With this notation, we obtain the following approximation for our main term. As the proof closely follows the arguments [BHB12, §8], we omit its details.

Lemma 6.1. *Assume that $H^{n_1 n_2/2} \leqslant V$ and $H^{n_1 n_2/2 - n_1/2} < V_0^{n_1}$. Then there is a constant ϑ_1 such that*

$$\mathscr{M}_{m, \mathbf{u}^{(m)}, \mathbf{v}^{(m)}, \mathbf{w}^{(m)}} = 2^\kappa M^{n_1} \sigma_\infty \tilde{\mathfrak{S}}^{(m)}(Q) + O_\eta\left(m^{\vartheta_1} Q^6 H^{n_1 n_2/2} V_0^{2n_1 n_2 + \eta}\right).$$

In this estimate one can take $\vartheta_1 = 3n_1 + 2n_2 + 1$.

It is now time to reintroduce the summation over d, e, f, k. Recalling the expression for $\mathscr{N}_\xi(G, H, V)$ in (4.6), and observing that

$$\mathscr{N}_{m, \mathbf{u}^{(m)}, \mathbf{v}^{(m)}, \mathbf{w}^{(m)}} = \mathscr{M}_{m, \mathbf{u}^{(m)}, \mathbf{v}^{(m)}, \mathbf{w}^{(m)}} + \mathscr{E}_{m, \mathbf{u}^{(m)}, \mathbf{v}^{(m)}, \mathbf{w}^{(m)}},$$

we assume that ξ is sufficiently small and that (5.2) holds. Then it follows from Lemma 5.4 that

$$
\mathscr{N}_\xi(G,H,V) = \sum_{\substack{d,e,f,k \leqslant V^\xi \\ (defk,Sv_0)=1}} \mu(d)\mu(e)\mu(f)\mu(k) \sum_{(\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}) \in \mathscr{S}(d,e,f,k)} \mathscr{M}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}}
$$
$$
+ O_\eta\left(Q^{-1/16} V^{7\xi(n_1+1)/2} V^{4\xi+7\xi(2n_1+n_2)} V_0^{2n_1 n_2 + O(\eta)} H^{n_1 n_2} \right),
$$

where we recall the notation (3.13) for Sv_0. We now use Lemma 6.1 to replace $\mathscr{M}_{m,\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}}$ with the expected approximation, giving

$$
\mathscr{N}_\xi(G,H,V) - \mathscr{N}_\xi^{(1)}(G,H,V)
$$
$$
\ll_\eta Q^{-1/16} V^{7\xi(n_1+1)/2} V^{4\xi+7\xi(2n_1+n_2)} V_0^{2n_1 n_2 + O(\eta)} H^{n_1 n_2} \tag{6.4}
$$
$$
+ V^{4\xi+7\xi(2n_1+n_2)} V^{7\xi\vartheta_1} Q^6 H^{n_1 n_2/2} V_0^{2n_1 n_2 + \eta},
$$

where

$$
\mathscr{N}_\xi^{(1)}(G,H,V) := \sum_{\substack{d,e,f,k \leqslant V^\xi \\ (defk,Sv_0)=1}} \mu(d)\mu(e)\mu(f)\mu(k)
$$
$$
\times \sum_{(\mathbf{u}^{(m)},\mathbf{v}^{(m)},\mathbf{w}^{(m)}) \in \mathscr{S}(d,e,f,k)} 2^\kappa M^{n_1} \sigma_\infty \tilde{\mathfrak{S}}^{(m)}(Q).
$$

We will be interested in triples of vectors $(\mathbf{p},\mathbf{q},\mathbf{s})$ such that

$$
(\mathbf{p},\mathbf{q},\mathbf{s}) \equiv (\mathbf{v}^{(M)},\mathbf{w}^{(M)},\mathbf{u}^{(M)}) \bmod M, \quad f^2 \mid c\,\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{q}), \tag{6.5}
$$
$$
[d^2,k] \mid N_{L/\mathbb{Q}}(\delta\,\mathbf{N}_{K_1/L}(\mathbf{s})), \quad [e^2,k] \mid N_{L/\mathbb{Q}}(\mathbf{N}_{K_1/L}(\mathbf{p})D_L). \tag{6.6}
$$

Letting $\Delta := [d^2,e^2,f^2,k,M,l,u]$, we define the counting function

$$
R(d,e,f,k,l,u) := \#\left\{ (\mathbf{p},\mathbf{q},\mathbf{s}) \bmod \Delta : (6.2),(6.5),(6.6) \text{ hold} \right\}. \tag{6.7}
$$

Then we have

$$
\mathscr{N}_\xi^{(1)}(G,H,V) = 2^\kappa M^{n_1} \sigma_\infty \sum_{\substack{d,e,f,k \leqslant V^\xi \\ (defk,Sv_0)=1}} \mu(d)\mu(e)\mu(f)\mu(k)
$$
$$
\times \sum_{q \leqslant Q} \sum_{l=1}^\infty \mu(l) \sum_{u \mid q} \frac{u\mu(q/u)}{\Delta^{2n_1+n_2}} R(d,e,f,k,l,u). \tag{6.8}
$$

We would next like to demonstrate the positivity of the sum over d,e,f,k,l and q. This is hampered by the presence of the Möbius functions and an important first step will be to show that the truncated sum in (6.8) can be completed. This is the object of the next section.

7. The singular series

In this section we continue our analysis of the sum (6.8) and then bring everything together in order to complete the proof of Theorem 4.3 (and so the proof of Theorem 1.2). We begin with a simple upper bound for the counting function (6.7), which does not exploit the congruence condition (6.2) modulo u, but is nonetheless useful when u is fixed.

Lemma 7.1. *Let* $\Delta = [d^2, e^2, f^2, k, M, l, u]$ *and let* $\eta > 0$. *Then*

$$R(d, e, f, k, l, u) \ll_\eta \frac{\Delta^{2n_1 + n_2}}{[d^2, k]^{1-\eta}[l^2, e^2, k]^{1-\eta} f^{2(1-\eta)}}.$$

Proof. Let $\Delta' := [d^2, e^2, f^2, k, M, l^2, u]$. Then $R(d, e, f, k, l, u)$ is at most

$$\left(\frac{\Delta}{\Delta'}\right)^{2n_1+n_2} \# \left\{ (\mathbf{p}, \mathbf{q}, \mathbf{s}) \bmod \Delta' : \begin{array}{c} [d^2, k] \mid N_{L/\mathbb{Q}}(\delta) \, \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{s}) \\ [l^2, e^2, k] \mid N_{L/\mathbb{Q}}(D_L) \, \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{p}) \\ f^2 \mid c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{q}) \end{array} \right\}.$$

The cardinality on the right hand side factors into three independent counting functions for $\mathbf{p}$, $\mathbf{q}$ and $\mathbf{s}$. By [BM15, Lemma 4.2] we have

$$\#\{\mathbf{p} \bmod \Delta' : [l^2, e^2, k] \mid N_{L/\mathbb{Q}}(D_L) \, \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{p})\} \ll_\eta \left(\frac{\Delta'}{[l^2, e^2, k]}\right)^{n_1} [l^2, e^2, k]^{n_1 - 1 + \eta}.$$

In a similar way one can estimate the contributions from $\mathbf{s}$ modulo Δ' with $[d^2, k] \mid N_{L/\mathbb{Q}}(\delta) \, \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{s})$, and $\mathbf{q}$ with $f^2 \mid c \, \mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{q})$. Together these bounds imply

$$R(d, e, f, k, l, u) \ll_\eta \frac{\Delta^{2n_1 + n_2}}{[d^2, k]^{1-\eta}[l^2, e^2, k]^{1-\eta} f^{2(1-\eta)}},$$

as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

In order to interpret the singular series we will need to complete the summation over q. Estimating the sum over $u \mid q$ trivially by taking absolute values of $\mu(q/u)$ does not suffice, even if the right decay for $R(d, e, f, k, l, u)$ is established, since the resulting majorant would not be convergent. Hence we proceed by consider the function

$$g(d, e, f, k, l, q) := \sum_{u \mid q} \frac{u \mu(q/u)}{\Delta^{2n_1 + n_2}} R(d, e, f, k, l, u),$$

where $R(d, e, f, k, l, u)$ is given by (6.7). Note that g and R implicitly depend on M. When we need to articulate the specific value of M, we will write g_M instead of g and R_M instead of R.

7.1. **Estimation of g.** Assume that we can write $d = d_1 d_2$, $e = e_1 e_2$, $f = f_1 f_2$, $k = k_1 k_2$, $l = l_1 l_2$, $q = q_1 q_2$ and $M = M_1 M_2$, with

$$(d_1 e_1 f_1 k_1 l_1 M_1 q_1, d_2 e_2 f_2 k_2 l_2 M_2 q_2) = 1.$$

Then the function g has the multiplicativity property

$$g_M(d, e, f, k, l, q) = g_{M_1}(d_1, e_1, f_1, k_1, l_1, q_1) g_{M_2}(d_2, e_2, f_2, k_2, l_2, q_2).$$

Hence it is sufficient to study $g_M(d, e, f, k, l, q)$ for values of M, d, e, f, k, l, q which are all powers of the same prime number p. Let $q = p^\alpha$ and assume now that M, d, e, f, k, l are powers of p. We write $\nu_p = \mathrm{val}_p$ for the standard p-adic valuation on $\mathbb{Q}$. In our study of the function g, we first consider the case where

$$\alpha + 1 \geqslant 2 \max\{\nu_p([d^2, k]), \nu_p([e^2, k]), \nu_p(f^2), \nu_p(l), \nu_p(M), 3/2\}. \tag{7.1}$$

For α in this range we have

$$g_M(d, e, f, k, l, p^\alpha) = \frac{p^\alpha}{p^{\alpha(2n_1 + n_2)}} R_M(d, e, f, k, l, p^\alpha)$$
$$- \frac{p^{\alpha-1}}{p^{(\alpha-1)(2n_1 + n_2)}} R_M(d, e, f, k, l, p^{\alpha-1}). \tag{7.2}$$

In the following we write $\mathbf{x}$ for the vector $(\mathbf{p}, \mathbf{q}, \mathbf{s})$ and define $F(\mathbf{x}) := F(\mathbf{p}, \mathbf{q}, \mathbf{s})$. Then (6.7) becomes

$$R_M(d, e, f, k, l, p^\alpha) = \#\left\{ \mathbf{x} \bmod p^\alpha : \begin{array}{l} F(\mathbf{x}) \equiv 0 \bmod p^\alpha, \ l \mid \mathbf{N}_{K_1/L}(\mathbf{p}) \\ (6.5), (6.6) \text{ hold} \end{array} \right\}.$$

For $\tau < \alpha$ we define the counting function

$$R_M^\tau(d, e, f, k, l, p^\alpha) = \#\left\{ \mathbf{x} \bmod p^\alpha : \begin{array}{l} F(\mathbf{x}) \equiv 0 \bmod p^\alpha, \ l \mid \mathbf{N}_{K_1/L}(\mathbf{p}) \\ p^\tau \| \nabla F(\mathbf{x}) \text{ and } (6.5), (6.6) \text{ hold} \end{array} \right\}.$$

Then $R_M(d, e, f, k, l, p^\alpha) = \sum_{\tau=0}^{\alpha-1} R_M^\tau(d, e, f, k, l, p^\alpha) + O(T(p^\alpha))$, where

$$T(p^t) := \#\{\mathbf{x} \bmod p^t : p^t \mid \nabla F(\mathbf{x})\}. \tag{7.3}$$

We now apply Hensel's lemma (in the form [BM15, Lemma 3.3], for example) in order to compare $R_M(d, e, f, k, l, p^\alpha)$ and $R_M(d, e, f, k, l, p^{\alpha-1})$. As soon as $\alpha - 1 \geqslant 2\tau + 1$ and

$$\alpha - 1 \geqslant \tau + \max\{\nu_p([d^2, k]), \nu_p([e^2, k]), \nu_p(f^2), \nu_p(l), \nu_p(M)\}, \tag{7.4}$$

we have $p^{2n_1 + n_2 - 1} R_M^\tau(d, e, f, k, l, p^{\alpha-1}) = R_M^\tau(d, e, f, k, l, p^\alpha)$. Note that the inequality $\alpha - 1 \geqslant 2\tau + 1$ is equivalent to saying that $\tau \leqslant \alpha/2 - 1$, from which it is clear that (7.1) implies (7.4). Together with equation (7.2) we obtain

$$g_M(d, e, f, k, l, p^\alpha) \ll \frac{p^\alpha}{p^{\alpha(2n_1 + n_2)}} \left(\frac{p^\alpha}{p^{\lfloor \frac{\alpha}{2} \rfloor}}\right)^{2n_1 + n_2} T(p^{\lfloor \frac{\alpha}{2} \rfloor}), \tag{7.5}$$

in the notation of (7.3). The function $T(p^t)$ has already been studied in [BHB12, §9], where the problem is reduced to the analysis of two independent counting functions T_1 and T_2, in such a way that $T(p^t) \leqslant T_1(p^t)T_2(p^t)$. It follows from [BHB12, Eq. (9.13) and p. 1186] that

$$T_1(p^t) \ll (4t+1)^{2n_1}p^{2n_1t - \lceil 2tn_1/(n_1-1)\rceil} \text{ and } T_2(p^t) \ll (2t+1)^{n_2}p^{n_2t - \lceil tn_2/(n_2-1)\rceil}.$$

This gives

$$T(p^t) \ll (4t+1)^{2n_1+n_2}p^{(2n_1+n_2)t-3t-2},$$

since $\lceil \theta \rceil \geqslant m+1$ for any real number θ bigger than an integer m. If we use this bound in (7.5), we obtain the estimate

$$g_M(d,e,f,k,l,p^\alpha) \ll (2\alpha+1)^{2n_1+n_2}p^{\alpha-3\lfloor\frac{\alpha}{2}\rfloor-2}.$$

By multiplicativity of g and using trivial bounds for $R_M(d,e,f,k,l,1)$, this estimate continues to hold for any positive integers M, d, e, f, k, l, which are not necessarily powers of p. We state this result in the following lemma.

Lemma 7.2. *Assume that* (7.1) *holds. Then*

$$g_M(d,e,f,k,l,p^\alpha) \ll \alpha^{2n_1+n_2}p^{\alpha-3\lfloor\frac{\alpha}{2}\rfloor-2}.$$

We will use this lemma later to handle cases where $\alpha \geqslant 3$, or $\alpha \geqslant 2$ and $p \nmid def$. It remains to bound the function g in situations where d, e, f, k, l are square-free, with either $\alpha = 1$, or $\alpha = 2$ and $p \mid def$. We begin by dealing with the latter situation.

Lemma 7.3. *Let $\eta > 0$. If $p \mid def$ then $g_M(d,e,f,k,l,p^2) \ll_\eta p^{-2+\eta}$.*

Proof. Suppose first that either $p^2 \mid de$, or $p \mid f$ and $p \mid dekl$, or $p^2 \mid f$. We use the definition of g in combination with the bound from Lemma 7.1 to deduce that

$$g_M(d,e,f,k,l,p^2) \ll p^2 \frac{R_M(d,e,f,k,l,p^2)}{\Delta(p^2)^{2n_1+n_2}} + p\frac{R_M(d,e,f,k,l,p)}{\Delta(p)^{2n_1+n_2}}$$
$$\ll_\eta p^2 p^{-4(1-\eta/4)} \ll_\eta p^{-2+\eta}.$$

Here we write $\Delta(p^2)$ and $\Delta(p)$ instead of Δ to indicate the dependence on u.

Next we consider the case $p \mid d$ and $p \nmid ef$. We take a similar strategy and note that the counting function $R_M(d,e,f,k,l,u)$ is

$$\leqslant \# \left\{ (\mathbf{p},\mathbf{q},\mathbf{s}) \bmod \Delta : \ p^2 \mid N_{L/\mathbb{Q}}(\delta)\,\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{s}), \ F(\mathbf{p},\mathbf{q},\mathbf{s}) \equiv 0 \bmod u \ \right\}.$$

In order to bound this counting function, we first count the number of possible choices for $\mathbf{s}$ modulo Δ. By [BM15, Lemma 4.2] one has

$$\#\{\mathbf{s} \bmod \Delta : p^2 \mid N_{L/\mathbb{Q}}(\delta)\,\mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{s})\} \ll_\eta \frac{\Delta^{n_1}}{p^{2-\eta/2}}.$$

Now consider $\mathbf{s}$ and $\mathbf{p}$ fixed and ask how many choices for $\mathbf{q}$ arise in the function $R_M(d, e, f, k, l, u)$. Again, we may apply [BM15, Lemma 4.2], concluding that

$$R(d, e, f, k, l, p^\alpha) \ll_\eta \frac{\Delta^{n_1}}{p^{2-\eta/2}} \Delta^{n_1} \frac{\Delta^{n_2}}{p^{\alpha-\eta/2}},$$

for $\alpha \in \{1, 2\}$. Hence the desired bound holds for $p \mid d$. The case $p \mid e$ may be treated in the same way.

It remains to bound the function g in the case $p \| f$ and $p \nmid dekl$. Since $(f, Sv_0) = 1$ we must have $p \nmid 2M$. Hence we need to analyse $g_1(1, 1, p, 1, 1, p^2)$. We proceed similarly to the proof of Lemma 7.2. Let

$$G(\mathbf{s}, \mathbf{p}) := \mathrm{Tr}_{L/\mathbb{Q}}(\delta \, \mathbf{N}_{K_1/L}(\mathbf{s}) \, \mathbf{N}_{K_1/L}(\mathbf{p}))$$

and define the counting function

$$\tilde{R}(u) := \#\{\mathbf{s}, \mathbf{p} \bmod u : G(\mathbf{s}, \mathbf{p}) \equiv 0 \bmod u\}.$$

Then $g_1(1, 1, p, 1, 1, p^2)$ is

$$= p^{-2(2n_1+n_2)}\big(p^2 R_1(1, 1, p, 1, 1, p^2) - p R_1(1, 1, p, 1, 1, p)\big)$$
$$= p^{-2(2n_1+n_2)}\#\{\mathbf{q} \bmod p^2 : p^2 \mid c\,\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{q})\}\big(p^2\tilde{R}(p^2) - p^{1+2n_1}\tilde{R}(p)\big).$$

Again we use [BM15, Lemma 4.2] to control the first counting function, obtaining

$$g_1(1, 1, p, 1, 1, p^2) \ll_\eta p^{-2+\eta}\big(p^{2-4n_1}\tilde{R}(p^2) - p^{1-2n_1}\tilde{R}(p)\big), \qquad (7.6)$$

for any $\eta > 0$. We further split the counting function $\tilde{R}(u)$ on prime powers $u = p^\alpha$ into two parts. Let

$$\tilde{R}_1(p^\alpha) := \#\{\mathbf{s}, \mathbf{p} \bmod p^\alpha : G(\mathbf{s}, \mathbf{p}) \equiv 0 \bmod p^\alpha, \ p \nmid \nabla G(\mathbf{s}, \mathbf{p})\}.$$

According to (7.6) we have

$$g_1(1, 1, p, 1, 1, p^2) \ll_\eta p^{-2+\eta}\big(p^{2-4n_1}\tilde{R}_1(p^2) - p^{1-2n_1}\tilde{R}_1(p)\big)$$
$$+ p^{-2+\eta}p^{2-2n_1}\#\{\mathbf{s}, \mathbf{p} \bmod p : p \mid \nabla G(\mathbf{s}, \mathbf{p})\}.$$

If we define $T_1(p^\tau)$ as in [BHB12, §9], then we see that

$$p^{2-2n_1}\#\{\mathbf{s}, \mathbf{p} \bmod p : p \mid \nabla G(\mathbf{s}, \mathbf{p})\} \ll p^{2-2n_1}T_1(p) \ll p^{2-\lceil 2n_1/(n_1-1)\rceil} \ll p^{-1},$$

and hence the second term is bounded by $O_\eta(p^{-3+\eta})$. Finally, it follows from [BM15, Lemma 3.3] that $p^{2-4n_1}\tilde{R}_1(p^2) = p^{1-2n_1}\tilde{R}_1(p)$, whence in this case $g_1(1, 1, p, 1, 1, p^2) \ll_\eta p^{-3+\eta}$. This completes the proof of the lemma. $\square$

Finally we turn to the case $\alpha = 1$.

Lemma 7.4. *Let $\eta > 0$. Then $g_M(d, e, f, k, l, p) \ll_\eta p^{-2+\eta}$.*

Proof. By using the trivial bound $R(d, e, f, k, l, u) \leqslant \Delta^{2n_1+n_2}$ and the multiplicativity of the function g, we may assume that all of d, e, f, k, l are powers of p. Moreover, since only finitely many primes p divide M, and our implicit constants may depend on M, we can assume that $M = 1$. Recall that

$$g_1(d, e, f, k, l, p) = p \frac{R_M(d, e, f, k, l, p)}{\Delta(p)^{2n_1+n_2}} - \frac{R_M(d, e, f, k, l, 1)}{\Delta(1)^{2n_1+n_2}}. \qquad (7.7)$$

If $p^3 \mid [d^2, k][l^2, e^2, k]f^2$, then the bound from Lemma 7.1 is already sufficient to establish the lemma. It remains to consider the following three cases.

Case (i): $p \nmid defkl$. In this case (7.7) becomes

$$g_1(1, 1, 1, 1, 1, p) = \frac{p}{p^{2n_1+n_2}} \#\{\mathbf{x} \bmod p : F(\mathbf{x}) \equiv 0 \bmod p\} - 1.$$

We shall count $\mathbb{F}_p$ points on the hypersurface $F = 0$, which has projective dimension $2n_1 + n_2 - 2$ and singular locus of projective dimension $2n_1 + n_2 - 7$. Hence we obtain

$$g_1(1, 1, 1, 1, 1, p) = \frac{p}{p^{2n_1+n_2}} (p^{2n_1+n_2-1} + O(p^{2n_1+n_2-3})) - 1 \ll p^{-2},$$

which is satisfactory.

Case (ii): $p \| defkl$. From Lemma 7.1 it is clear that

$$\frac{R_M(d, e, f, k, l, 1)}{\Delta(1)^{2n_1+n_2}} \ll_\eta p^{-2+\eta}.$$

We start with the case that $d = p$, observing that $p \nmid N_{L/\mathbb{Q}}(\delta)$ since $(d, S) = 1$. In this case $R_1(p, 1, 1, 1, 1, p)$ is equal to

$$\#\{(\mathbf{p}, \mathbf{q}, \mathbf{s}) \bmod p^2 : p^2 \mid \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{s}), \ F(\mathbf{p}, \mathbf{q}, \mathbf{s}) \equiv 0 \bmod p\}.$$

To estimate this, we first sum over all $\mathbf{s}$ modulo p^2 with $p^2 \mid \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{s})$, and then fix some arbitrary $\mathbf{p}$ modulo p^2. For such a tuple, one again needs to estimate the number of solutions to $\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{q}) \equiv \mu$ modulo p for some residue μ modulo p. Two applications of [BM15, Lemma 4.2] lead to the bound

$$R(p, 1, 1, 1, 1, p) \ll_\eta p^{2(2n_1+n_2)} p^{-2+\eta/2} p^{-1+\eta/2} \ll_\eta p^{2(2n_1+n_2)-3+\eta}.$$

Hence we deduce from (7.7) that $g_1(p, 1, 1, 1, 1, p) \ll_\eta p^{-2+\eta}$, as desired. The estimates for the other cases where p divides exactly one of e, f, k, l are established in the same way.

Case (iii): $p \mid l$ and $p \mid e$ and $p \nmid dfk$. The same arguments as above leads to the estimate

$$R_1(1, p, 1, 1, p, p) \ll \#\{\mathbf{x} \bmod p^2 : p^2 \mid \mathbf{N}_{K_1/\mathbb{Q}}(\mathbf{p}), \ F(\mathbf{x}) \equiv 0 \bmod p\} \ll_\eta p^{-3+\eta},$$

and $R_1(1, p, 1, 1, p, 1) \ll_\eta p^{-2+\eta}$. Once combined with (7.7), this is enough to establish the lemma. $\square$

7.2. **Absolute convergence of the singular series.** We have now collected all the bounds that we need to show that one may complete the summations over d, e, f, k, q in the definition of $N_\xi^{(1)}(G, H, V)$ in (6.8). Observe that

$$\sum_{\substack{d,e,f,k \leqslant V^\xi \\ (defk,Sv_0)=1}} |\mu(d)\mu(e)\mu(f)\mu(k)| \sum_{q \leqslant Q} \sum_{l=1}^{\infty} |\mu(l)||g_M(d,e,f,k,l,q)|$$

$$\ll \prod_p \left(\sum_{\alpha_1,\ldots,\alpha_5 \in \{0,1\}} \sum_{\beta=0}^{\infty} |g_{p^{\nu_p(M)}}(p^{\alpha_1}, \ldots, p^{\alpha_5}, p^\beta)| \right),$$

where the product over p is taken over all prime numbers. We define

$$\mathfrak{S} := \sum_{\substack{d,e,f,k \in \mathbb{N} \\ (defk,Sv_0)=1}} \sum_{l=1}^{\infty} \mu(d)\mu(e)\mu(f)\mu(k)\mu(l) \sum_{q=1}^{\infty} g_M(d,e,f,k,l,q).$$

The following lemma shows that $\mathfrak{S}$ is indeed absolutely convergent.

Lemma 7.5. *For any prime p one has*

$$\sum_{\alpha_1,\ldots,\alpha_5 \in \{0,1\}} \sum_{\beta=0}^{\infty} |g_{p^{\nu_p(M)}}(p^{\alpha_1}, \ldots, p^{\alpha_5}, p^\beta)| = p^{-\nu_p(M)(2n_1+n_2)}\left(1 + O_\eta(p^{-2+\eta})\right),$$

where the implied constant depends only on η and M.

Proof. It is easy to see that $g_{p^{\nu_p(M)}}(1, \ldots, 1) = p^{-\nu_p(M)(2n_1+n_2)}$. Hence we need to show that the contribution from the remaining summands is $O_\eta(p^{-2+\eta})$. For $\beta = 0$ and $\sum_{i=1}^{5} \alpha_i \geqslant 1$, Lemma 7.1 shows that

$$g_{p^{\nu_p(M)}}(p^{\alpha_1}, \ldots, p^{\alpha_5}, 1) \ll_\eta p^{-2+\eta}.$$

Furthermore, Lemma 7.4 implies that

$$\sum_{\alpha_1,\ldots,\alpha_5 \in \{0,1\}} |g_{p^{\nu_p(M)}}(p^{\alpha_1}, \ldots, p^{\alpha_5}, p)| \ll_\eta p^{-2+\eta},$$

which corresponds to the terms with $\beta = 1$. For $\beta = 2$ and $\alpha_1 + \alpha_2 + \alpha_3 \geqslant 1$, one may use Lemma 7.3 to bound these terms by $O_\eta(p^{-2+\eta})$, and for $\beta = 2$ and $\alpha_1 = \alpha_2 = \alpha_3 = 0$, the same bound follows from Lemma 7.2. We finally apply Lemma 7.2 to estimate the contribution from $\beta \geqslant 3$ by

$$\sum_{\alpha_1,\ldots,\alpha_5 \in \{0,1\}} \sum_{\beta=3}^{\infty} |g_{p^{\nu_p(M)}}(p^{\alpha_1}, \ldots, p^{\alpha_5}, p^\beta)| \ll \sum_{\beta=3}^{\infty} \beta^{2n_1+n_2} p^{\beta-3\lfloor\frac{\beta}{2}\rfloor-2} \ll p^{-2}.$$

This completes the proof of the lemma. $\qquad\square$

We now factorise $\mathfrak{S}$ into a product of local densities. For $p \nmid Sv_0$ we define

$$\sigma_p := \sum_{\alpha_1,\dots,\alpha_5 \in \{0,1\}} (-1)^{\sum_{i=1}^{5} \alpha_i} \sum_{\beta=0}^{\infty} g_1(p^{\alpha_1}, \dots, p^{\alpha_5}, p^{\beta}),$$

and for $p \mid Sv_0$ we set

$$\sigma_p := \sum_{\alpha \in \{0,1\}} (-1)^{\alpha} \sum_{\beta=0}^{\infty} g_{p^{\nu_p(M)}}(1, 1, 1, 1, p^{\alpha}, p^{\beta}).$$

We have $\mathfrak{S} = \prod_p \sigma_p$, since $\mathfrak{S}$ is absolutely convergent. In order to show that $\mathfrak{S}$ is positive, it will therefore be sufficient to show that each of the factors σ_p is positive.

Note that $\sigma_p = \lim_{T \to \infty} \sigma_p(T)$, with

$$\sigma_p(T) := \sum_{\alpha_1,\dots,\alpha_5 \in \{0,1\}} (-1)^{\sum_{i=1}^{5} \alpha_i} \sum_{\beta=0}^{T} g_{p^{\nu_p(M)}}(p^{\alpha_1}, \dots, p^{\alpha_5}, p^{\beta}),$$

in the case $p \nmid Sv_0$, and in a similar way for $p \mid Sv_0$. We rewrite $\sigma_p(T)$ as

$$\sigma_p(T) = \sum_{\alpha_1,\dots,\alpha_5 \in \{0,1\}} (-1)^{\sum_{i=1}^{5} \alpha_i} \left(\frac{1}{\Delta(1)^{2n_1+n_2}} R_{p^{\nu_p(M)}}(p^{\alpha_1}, \dots, p^{\alpha_5}, 1) \right.$$

$$+ \sum_{\beta=1}^{T} \frac{p^{\beta}}{\Delta(p^{\beta})^{2n_1+n_2}} R_{p^{\nu_p(M)}}(p^{\alpha_1}, \dots, p^{\alpha_5}, p^{\beta})$$

$$\left. - \sum_{\beta=1}^{T} \frac{p^{\beta-1}}{\Delta(p^{\beta-1})^{2n_1+n_2}} R_{p^{\nu_p(M)}}(p^{\alpha_1}, \dots, p^{\alpha_5}, p^{\beta-1}) \right).$$

We recognise the summation in β as a telescoping sum for each fixed vector $(\alpha_1, \dots, \alpha_5)$. For T sufficiently large, we therefore obtain

$$\sigma_p(T) = \sum_{\alpha_1,\dots,\alpha_5 \in \{0,1\}} (-1)^{\sum_{i=1}^{5} \alpha_i} \frac{p^T}{p^{T(2n_1+n_2)}} R_{p^{\nu_p(M)}}(p^{\alpha_1}, \dots, p^{\alpha_5}, p^T),$$

which we can interpret as a normalised counting function modulo p^T. To be precise, for $p \mid Sv_0$ and $T \geqslant \max\{2, \nu_p(M)\}$ define $\mathscr{R}(p^T)$ to be the number of vectors $\mathbf{x}$ modulo p^T that satisfy

$$(\mathbf{p}, \mathbf{q}, \mathbf{s}) \equiv (\mathbf{v}^{(M)}, \mathbf{w}^{(M)}, \mathbf{u}^{(M)}) \bmod p^{\nu_p(M)}, \qquad p \nmid \mathbf{N}_{K_1/L}(\mathbf{p}), \tag{7.8}$$

and

$$F(\mathbf{x}) \equiv 0 \bmod p^T.$$

For $p \nmid Sv_0$ we define $\mathscr{R}(p^T)$ in the same way, but with the additional restrictions that

$$p^2 \nmid N_{L/\mathbb{Q}}(\delta\,\mathbf{N}_{K_1/L}(\mathbf{s})), \quad p^2 \nmid N_{L/\mathbb{Q}}(\mathbf{N}_{K_1/L}(\mathbf{p})D_L), \quad p^2 \nmid c\,\mathbf{N}_{K_2/\mathbb{Q}}(\mathbf{q}),$$

$$p \nmid \left(N_{L/\mathbb{Q}}(\delta\,\mathbf{N}_{K_1/L}(\mathbf{s})), N_{L/\mathbb{Q}}(\mathbf{N}_{K_1/L}(\mathbf{p})D_L)\right). \tag{7.9}$$

Then for $T \geqslant \max\{2, \nu_p(M)\}$ one has the expression

$$\sigma_p(T) = \frac{p^T}{p^{T(2n_1+n_2)}}\mathscr{R}(p^T).$$

7.3. **Completion of the proof.** We now have everything in place to show that

$$\mathfrak{S} > 0. \tag{7.10}$$

Our work in the previous section shows that it suffices to show that $\sigma_p > 0$ for every prime p. It is clearly sufficient to find a smooth p-adic solution to $F(\mathbf{x}) = 0$, that satisfies the additional congruence conditions (7.8) in the case $p \mid Sv_0$, and both (7.8) and (7.9) for $p \nmid Sv_0$. For $p \nmid M$, it is sufficient to find a non-singular solution to $F(\mathbf{x}) = 0$ over $\mathbb{F}_p$, such that $p \nmid \mathbf{N}_{K_1/L}(\mathbf{p})$ and p divides none of the expressions in (7.9).

As in [BHB12, §9], we observe that the equation $F(\mathbf{x}) = 0$ has

$$p^{2n_1+n_2-1} + O(p^{2n_1+n_2-3})$$

solutions over $\mathbb{F}_p$. The number of solutions with any of the additional restrictions $p \mid \mathbf{N}_{K_1/L}(\mathbf{p})$, or p divides one of the expressions in (7.9), or $\mathbf{x}$ is a singular point of $F(\mathbf{x}) = 0$, is bounded by $O(p^{2n_1+n_2-2})$. Hence, for $p \geqslant p_0$, there is a non-singular solution to $F(\mathbf{x}) = 0$ over $\mathbb{F}_p$, such that $p \nmid \mathbf{N}_{K_1/L}(\mathbf{p})$ and p divides none of the expressions in (7.9). This solution may be lifted via Hensel's lemma and shows that $\sigma_p > 0$ for $p \geqslant p_0$.

We may assume without loss of generality that all primes $p < p_0$ are contained in $S_f \cup \{v_0\}$. For $p \mid M$, we recall that we have set $\mathbf{v}^{(M)} = (1, 0, \ldots, 0)$. By Lemma 3.1, for any prime $p \in S_f$, we are given a solution $(\mathbf{y}_p, \mathbf{w}_p) \in \mathscr{W}(\mathbb{Z}_p)$ with $(\mathbf{y}_p, \mathbf{w}_p) \equiv (\mathbf{y}^{(M)}, \mathbf{w}^{(M)})$ modulo M. Since $\mathscr{W}$ is non-singular, this is already enough to establish $\sigma_p > 0$ for $p \in S_f$. It remains to consider the prime p_0 corresponding to v_0 if this is a finite place. In the beginning of the argument we may assume that we are given some p_0-adic solution to $F(\mathbf{x}) = 0$ with $\mathbf{p} = (1, 0, \ldots, 0)$. After renormalising we may even assume that this is an integral p_0-adic solution. Again since W is smooth, this is sufficient to show that $\sigma_{p_0} > 0$, which thereby concludes the proof of (7.10).

We now turn our attention to the singular integral (6.3). For G sufficiently large, the domains $\mathscr{V}$ and $\mathscr{W}$ coincide with those defined in [BHB12]. Moreover, our singular integral σ_∞ is up to two fixed normalisation constants (M_1^n and c) the same as that defined in [BHB12]. Hence their arguments apply

and show that $\sigma_\infty \gg G^{1-2n_1-n_2} H^{n_1 n_2} V_0^{2n_1 n_2}$. The lower bounds for $\mathfrak{S}$ and σ_∞ in combination with (6.8) and the fact that $\mathfrak{S}$ is absolutely convergent, now show that

$$\mathscr{N}_\xi^{(1)}(G, H, V) \gg G^{1-2n_1-n_2} H^{n_1 n_2} V_0^{2n_1 n_2}. \tag{7.11}$$

We now set $G = \log V$ and $H = V^{\frac{1}{n_1 n_2^2 (n_1 + 16)}}$. Recalling (4.2), these choices clearly imply that $H^{n_1 n_2 / 2} \leqslant V$ and $H^{n_1 n_2 / 2 - n_1 / 2} < V_0^{n_1}$; i.e. the assumptions of Lemma 6.1 are satisfied. We choose Q a fixed small power of H such that $Q^6 < H^{n_1 n_2 / 4}$ and (5.2) holds. Take ξ sufficiently small. Then we may combine (6.4) with (4.4) and the lower bound (7.11) to complete the proof of Theorem 4.3.

References

[BHB12] T.D. Browning and D.R. Heath-Brown, Quadratic polynomials represented by norm forms. *GAFA* **22** (2012), 1124–1190.

[BM15]   T.D. Browning and L. Matthiesen, Norm forms for arbitrary number fields as products of linear polynomials. *Ann. Sci. Éc. Norm. Sup.* **50**, 2017, 1375–1438.

[CTS00] J.-L. Colliot-Thélène and A. Skorobogatov, Descent on fibrations over $\mathbb{P}_k^1$ revisited. *Math. Proc. Camb. Phil. Soc.* **128** (2000), 383–393.

[CTX13] J.-L. Colliot-Thélène and F. Xu, Strong approximation for the total space of certain quadric fibrations. *Acta Arithmetica* **157** (2013), 169–199.

[DSW15] U. Derenthal, A. Smeets and D. Wei, Universal torsors and values of quadratic polynomials represented by norms. *Math. Annalen* **361** (2015), 1021–1042.

[Har97] D. Harari, Flèches de spécialisations en cohomologie étale et applications arithmétiques. *Bull. Soc. Math. France* **125** (1997), 143–166.

[HW15]   Y. Harpaz and O. Wittenberg, On the fibration method for zero-cycles and rational points. *Annals of Math.* **183** (2016), 229–295.

[Mat15] L. Matthiesen, On the square-free representation function of a norm form and nilsequences. *J. Inst. Math. Jussieu*, to appear.

[San81] J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, *J. reine angew. Math.* **327** (1981), 12–80.

[Sko96] A.N. Skorobogatov, Descent over the fibrations over the projective line. *Amer. J. Math.* **118** (1996), 905–923.

School of Mathematics, University of Bristol, Bristol, BS8 1TW, UK
E-mail address: t.d.browning@bristol.ac.uk

Utrecht University, Hans Freudenthalgebouw, Budapestlaan 6, 3584 CD Utrecht, Netherlands
E-mail address: d.schindler@uu.nl