Chapter 3

The density of fibres with a rational point for a fibration over hypersurfaces of low degree

A victory is twice itself when the achiever brings home full numbers

Leonato, Much Ado About Nothing, Scene 1.1, line 5

This chapter is an adapted version of a paper that is being prepared jointly with Efthymios Sofos, and for which a preprint is available online [SVM18].

3.1 Introduction

Serre's problem [Ser90] regards the density of elements in a family of varieties defined over $\mathbb{Q}$ that have a $\mathbb{Q}$-rational point. Special cases have been considered by Hooley [Hoo93, Hoo07] Poonen–Voloch [PV04], Sofos [Sof16], Browning–Loughran [BL17], and Loughran–Takloo-Bighash–Tanimoto [LTBT17]. The recent investigation of Loughran [Lou13] and Loughran–Smeets [LS16] provides an appropriate formulation of the problem and proves the conjectured upper bound in considerable generality.

Assume that X is a variety over $\mathbb{Q}$ equipped with a dominant morphism $\phi : X \to \mathbb{P}^n_{\mathbb{Q}}$. Letting H denote the usual Weil height on $\mathbb{P}^n(\mathbb{Q})$, Loughran and Smeets conjectured [LS16, Conj.1.6] under suitable assumptions on ϕ, that for all large enough positive t, the cardinality of points $b \in \mathbb{P}^n(\mathbb{Q})$

with height $H(b) \leq t$ and such that the fibre $\phi^{-1}(b)$ has a point in $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p, has order of magnitude

$$\frac{\#\{b \in \mathbb{P}^n(\mathbb{Q}) : H(b) \leq t\}}{(\log t)^{\Delta(\phi)}}$$

for a non-negative quantity $\Delta(\phi)$ that is defined in [LS16, Eq.(1.3)].

The cardinality of fibres of height t and possessing a $\mathbb{Q}$-rational point is bounded by the quantity they considered, while the two quantities coincide if every fibre satisfies the Hasse principle. The problem of obtaining the conjectured lower bound for the number of fibres of bounded height with a $\mathbb{Q}$-rational point when ϕ is general is considered rather hard because there is no general machinery for producing $\mathbb{Q}$-rational points on varieties.

There are only two instances in the literature of the subject where asymptotics have been proved unconditionally:

- the base of the fibration is a toric variety (Loughran [Lou13]),
- the base of the fibration is a wonderful compactification of an adjoint semi-simple algebraic group (Loughran–Takloo-Bighash–Tanimoto [LTBT17]).

Our aim in this chapter is to extend the list above by proving asymptotics in a case of a rather different nature. The base of the fibration of our main theorem will be a generic hypersurface of large dimension compared to its degree.

3.1.1 The set-up of our results

Let f_1 and f_2 be homogeneous forms in $\mathbb{Z}[t_0, \ldots, t_{n-1}]$, of equal and even degree $d > 0$ subject to some assumptions which are to follow.

We assume that both the projective varieties defined by $f_1(\mathbf{t}) = 0$ and $f_2(\mathbf{t}) = 0$ are smooth. Moreover we assume that the variety defined by $f_1(\mathbf{t}) = f_2(\mathbf{t}) = 0$ is a complete intersection. This is satisfied for generic f_1 and f_2 of fixed degree and in a fixed number of variables. The next condition is artificial in nature but its presence allows to adapt the arguments of Birch [Bir62] to our problem. Letting $\sigma(f_1, f_2)$ denote the dimension of the variety given by

$$\operatorname{rk}\left(\frac{\partial f_i}{\partial x_j}\right)_{0\leq j\leq n-1}^{1\leq i\leq 2}(\mathbf{x}) \leq 1$$

when considered as a subvariety in $\mathbb{A}^n_{\mathbb{C}}$, we shall demand the validity of

$$n - \sigma(f_1, f_2) > 3(d-1)2^d. \tag{3.1}$$

With more work along the lines of the present chapter, most of these assumptions may be removed. However, the assumption that $\deg(f_1)$ is even seems necessary and (3.1) is vital for the entire strategy of the proof. We discuss some possible adaptations after stating the main result of our work.

Remark 3.1.1. We assume that the varieties defined by $f_i(\mathbf{t}) = 0$ are smooth, so they are also irreducible since smooth hypersurfaces in $\mathbb{P}^{n-1}_{\mathbb{Q}}$ are irreducible if $n \geq 3$ holds. In particular we have $n > 12$ by (3.1).

Let $B \subset \mathbb{P}^{n-1}_{\mathbb{Q}}$ be the hypersurface given by $f_2(\mathbf{t}) = 0$. We recall that by the work of Birch [Bir62], B satisfies the Hasse principle, and moreover it satisfies weak approximation by work of Browning and Heath-Brown [BHB17]. From now on we also assume $B(\mathbb{Q}) \neq \emptyset$.

For every $i \in \{0, \dots, n-1\}$ consider the subvariety X_i of $\mathbb{P}^2_{\mathbb{Q}} \times \mathbb{A}^{n-1}_{\mathbb{Q}}$ defined by

$$\begin{aligned} x_0^2 + x_1^2 =& f_1(t_0, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_{n-1}) x_2^2, \\ & f_2(t_0, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_{n-1}) = 0. \end{aligned}$$

The maps $g_i : X_i \to B \subset \mathbb{P}^{n-1}_{\mathbb{Q}}$ sending a pair

$$((x : y : z), (t_0, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_{n-1}))$$

to $(t_0 : \dots : t_{i-1} : 1 : t_{i+1} : \dots : t_{n-1})$ glue together, defining a projective bundle X over the base B – this uses that f_1 has even degree. By assumption, f_1 is not a multiple of f_2, so the generic fibre of X is smooth.

If we were interested in counting $\mathbb{Q}$-rational points on X then it would be necessary to make a further study into the equations defining a projective embedding of X (as in [FLS18, §2]). Currently however, we are only interested in counting how many fibres of the conic bundle have a $\mathbb{Q}$-rational point. A *conic bundle* is a dominant morphism whose generic fibre is a smooth conic. In this chapter we consider the conic bundle

$$\phi : X \to B \tag{3.2}$$

defined locally by g_i. We shall estimate asymptotically the probability with which the fibre $\phi^{-1}(b)$ has a $\mathbb{Q}$-point as b ranges over $B(\mathbb{Q})$. For this, we define

$$N(\phi, t) := \#\big\{b \in B(\mathbb{Q}) : H(b) \leq t,\ b \in \phi(X(\mathbb{Q}))\big\},\ t \in \mathbb{R}_{>0},$$

where H is the usual naive Weil height on $\mathbb{P}^{n-1}(\mathbb{Q})$.

Remark 3.1.2. Since the degree of f_1 is even, the question if for a given $b \in B$ the fibre $\phi^{-1}(b)$ contains a rational point is independent of a chosen representative.

Consider the small quantity

$$\varepsilon_d := \frac{1}{5(d-1)2^{d+5}}. \tag{3.3}$$

Theorem 3.1.3. *In the set-up above there exists a constant c_ϕ such that for $t \geq 2$ we have*

$$N(\phi, t) = c_\phi \frac{t^{n-d}}{(\log t)^{\frac{1}{2}}} + O\left(\frac{t^{n-d}}{(\log t)^{\frac{1}{2}+\varepsilon_d}}\right).$$

If ϕ has a smooth fibre with a $\mathbb{Q}$-point then c_ϕ is positive. This will be shown in Theorem 3.5.23, where we shall also provide an interpretation for the leading constant c_ϕ. The proof of Theorem 3.1.3 will be given in §3.4.3.

In fact, the assumption that the base B has a rational point could be removed, as Theorem 3.5.23 will show that in this case, the constant c_ϕ would vanish. It is however convenient for our methods to keep the assumption anyway. And indeed, if $B(\mathbb{Q})$ were empty, the study of $N(\phi, t)$ would be a trivial exercise.

Theorem 3.1.3 settles the first case in the literature of an asymptotic for the natural extension of Serre's problem to fibrations over a base that does not have the structure of a toric variety nor a wonderful compactification of an adjoint semi-simple algebraic group. Fibrations that have a basis other than the projective space were also studied in the recent work of Browning and Loughran [BL17, §1.2.2]. In light of the work of Birch [Bir62], our assumptions imply

$$\#\big\{b \in B(\mathbb{Q}) : H(b) \leq t\big\} \asymp t^{n-d}.$$

A very special case of [BL17, Thm 1.4] proves $\lim_{t\to\infty} N(\phi, t)/t^{n-d} = 0$, whereas Theorem 3.1.3 provides asymptotics.

The requirements $\deg(f_1) = \deg(f_2)$ and that the variety $f_1(\mathbf{t}) = f_2(\mathbf{t}) = 0$ is a complete intersection can be removed by adapting some of the arguments in the work of Browning and Heath-Brown [BHB17]. An inspection of our work reveals that the smoothness assumption can be removed at the cost of making the statement Theorem 3.1.3 more involved. Lastly, we should note that our approach can be adapted to varieties of the form $(\mathrm{N}_{K/\mathbb{Q}}(\mathbf{x}) = f_1(b),\ f_2(b) = 0)$, where K is a number field and $\mathrm{N}_{K/\mathbb{Q}}(\mathbf{x})$ is the associated norm form. For this, one would have to replace Proposition 3.3.4 by a version of the results of Odoni [Odo73], where instead of counting integers represented by the norm of K, one counts integers in an arbitrary arithmetic progression and represented by the norm of K. It would be interesting to obtain asymptotics in cases where K fails the Hasse norm principle. A further desirable goal could be that of obtaining asymptotics in cases where the base of the fibration fails weak approximation.

3.1.2 The logarithmic exponent

The exponent of $\log t$ occurring in our result is the one expected in the literature. Indeed, in the works of Loughran and Smeets [LS16, Eq.(1.4)], and Browning and Loughran [BL17, Eq.(1.3)], one may find the expected exponent $\Delta(\phi)$ defined as follows. For any $b \in B$ with residue field $\kappa(b)$, the fibre $X_b = \phi^{-1}(b)$ is called *pseudo-split* if every element of $\mathrm{Gal}(\overline{\kappa(b)}/\kappa(b))$ fixes some multiplicity-one irreducible component of $X_b \times \mathrm{Spec}(\overline{\kappa(b)})$. The fibre X_b is called *split* if it contains a multiplicity-one irreducible component that is also geometrically irreducible. Note that a split fibre is always pseudo-split and further note that for conic bundles these two notions are the same as the singular fibres are either double lines, or two lines intersecting.

Now for every codimension one point $D \in B^{(1)}$ choose a finite group Γ_D through which the action of $\mathrm{Gal}(\overline{\kappa(D)}/\kappa(D))$ on the irreducible components of $X_{\overline{\kappa(D)}}$ factors. Let Γ_D° be the subset of elements of Γ_D which fix some multiplicity one irreducible component. One sets $\delta_D = \#\Gamma_D^\circ/\#\Gamma_D$ and

$$\Delta(\phi) = \sum_{D\in B^{(1)}} \big(1 - \delta_D\big).$$

By considering the possible singular fibres, it is clear that for a conic bundle, δ_D is different from 1 if and only if D is non-split, in which case it is either 0 (if the fibre is a double line) or $\frac{1}{2}$.

In all the cases in the literature so far the exponent of $(\log t)^{-1}$ turns out to be Δ. Indeed, this is also the case here. The only relevant codimension one point to consider is $D := Z(f_1, f_2)$; every other fibre is smooth and hence split. Suppose that D is geometrically reducible, then the intersection between any two geometrically irreducible components lies in the singular locus of D, say D^{sing}. Being the intersection between varieties in projective space of codimension at most 2, its codimension is at most 4.

The affine cone above D^{sing} is a subvariety of the affine variety defined by

$$\mathrm{rk}\left(\frac{\partial f_i}{\partial x_j}\right)_{0\leq j\leq n-1}^{1\leq i\leq 2}(\mathbf{x}) \leq 1.$$

As a subvariety, the affine cone over D^{sing} has dimension at most $\sigma(f_1, f_2)$, so its codimension is at least $n-\sigma(f_1, f_2)$. Hence the codimension of D^{sing} in $\mathbb{P}^n_{\mathbb{Q}}$ is at least $n - \sigma(f_1, f_2) - 1$. Thus we are led to an inequality

$$4 \geq n - \sigma(f_1, f_2) - 1 > 3(d-1)2^d - 1 \geq 11,$$

violating the combined assumptions (3.1) and $d \geq 2$. We conclude that D is geometrically irreducible.

The fibre above D is given by $x^2+y^2 = 0$ over the function field $\kappa(D)$ and it is split if and only if -1 is a square in $\kappa(D)$. However, it is well known that the function field of a geometrically irreducible variety is primary: it contains no non-trivial separable algebraic extensions of the base field. Since -1 is not a square in $\mathbb{Q}$, neither is it in $\kappa(D)$. Therefore, under the assumptions of Theorem 3.1.3 we find $\Delta(\phi) = \delta_D = \frac{1}{2}$.

NOTATION 3.1.4. As usual, we denote the divisor, Euler and Möbius functions by τ, φ and μ. We shall make frequent use of the estimates

$$\tau(m) \ll m^{\frac{1}{\log\log m}} \tag{3.4}$$

and

$$\varphi(m) \gg m/\log\log m \tag{3.5}$$

found in [Ten95, Th.5.4] and [Ten95, Th.5.6] respectively.

We consider the forms f_1 and f_2 fixed throughout the chapter, thus the implied constants in the Vinogradov/Landau notation $\ll$, $O(\cdot)$ are allowed to depend on ϕ, f_1, f_2, n and d without further mention. Any dependence of the implied constants on other parameters will be explicitly recorded by the appropriate use of a subscript.

For $z \in \mathbb{C}$ we let

$$\mathrm{e}(z) := \exp(2\pi i z).$$

The symbol $v_p(m)$ will refer to the standard p-adic valuation of an integer m. Lastly, we shall use the Ramanujan sum, defined for $a \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$ as

$$c_q(a) := \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^*} \mathrm{e}(ax/q). \tag{3.6}$$

Denoting the indicator function of a condition A by $\mathbf{1}_A$, we have the following equality:

$$c_{p^m}(a) = p^{m-1}\big(p\mathbf{1}_{v_p(a)\geq m} - \mathbf{1}_{v_p(a)\geq m-1}\big), \ (p \text{ prime}, a \in \mathbb{Z}, m \geq 1). \tag{3.7}$$

When we write $|\mathbf{x}|$, we will mean $\max\{|x_i|\}$. Lastly, we shall make frequent use of the constant

$$\mathcal{C}_0 := \prod_{\substack{p \text{ prime} \\ p \equiv 3 (\mathrm{mod}\ 4)}} \Big(1 - \frac{1}{p^2}\Big)^{1/2}. \tag{3.8}$$

Acknowledgements This work started while Efthymios Sofos had a position at Leiden University. It was completed while Erik Visse–Martindale was visiting the Max Planck Institute in Bonn, the hospitality of which is greatly acknowledged. The authors are very grateful to Daniel Loughran for useful comments that helped improve the introduction and §3.5.4.

3.2 Using the Hardy–Littlewood circle method for Serre's problem

We begin by estimating the main quantity in Theorem 3.1.3 by averages of an arithmetic function over a thin subset of integer vectors. Let us first define $\vartheta_{\mathbb{Q}} : \mathbb{Z} \to \{0, 1\}$ as the indicator function of those integers m such

that the curve $x_0^2 + x_1^2 = mx_2^2$ has a point over $\mathbb{Q}$. For $P \in \mathbb{R}_{>0}$ we let

$$\Theta_{\mathbb{Q}}(P) := \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \cap P[-1,1]^n \\ f_1(\mathbf{x}) \neq 0, f_2(\mathbf{x}) = 0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{x})). \tag{3.9}$$

In order to go from $\mathbb{Q}$-solutions to coprime $\mathbb{Z}$-solutions, we perform a standard Möbius transformation, where we cut off the range of summation at the price of an error term. This is the content of the following lemma.

LEMMA 3.2.1. *Under the assumptions of Theorem 3.1.3 we have*

$$N(\phi, t) = \frac{1}{2} \sum_{l \in \mathbb{Z} \cap [1, \log t]} \mu(l) \Theta_{\mathbb{Q}}(t/l) + O(t^{n-d} (\log t)^{-1}).$$

Proof. For any $b \in \mathbb{P}^n(\mathbb{Q})$ there exists a unique, up to sign, $\mathbf{y} \in \mathbb{Z}^n$ with $\gcd(y_0, \ldots, y_{n-1}) = 1$ and $b = [\pm \mathbf{y}]$. Recalling that the degree of f_1 is even, allows to infer that the fibre $\phi^{-1}(b)$ has a rational point if and only if $\vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) = 1$ holds, hence $N(\phi, t)$ equals

$$\frac{1}{2} \#\{\mathbf{y} \in \mathbb{Z}^n \cap t[-1,1]^n : \gcd(y_0, \ldots, y_{n-1}) = 1, f_2(\mathbf{y}) = 0, \vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) = 1\}.$$

For $\mathbf{y}$ such that $f_1(\mathbf{y}) = 0$ holds, we have $\vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) = 1$ since $(0:0:1)$ is a point in $\phi^{-1}([\mathbf{y}])$. Therefore the quantity above is

$$\frac{1}{2} \sum_{\substack{\mathbf{y} \in \mathbb{Z}^n \cap t[-1,1]^n \\ \gcd(y_0, \ldots, y_{n-1}) = 1 \\ f_2(\mathbf{y}) = 0, f_1(\mathbf{y}) \neq 0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) + O(\#\{\mathbf{y} \in \mathbb{Z}^n \cap [-t,t]^n : f_1(\mathbf{y}) = f_2(\mathbf{y}) = 0\}).$$

The assumption (3.1) allows to apply Lemma 1.3.36 with $R = 2$ to immediately obtain

$$\#\{\mathbf{y} \in \mathbb{Z}^n \cap t[-1,1]^n : f_1(\mathbf{y}) = f_2(\mathbf{y}) = 0\} \ll t^{n-2d}.$$

Thus we obtain equality of $N(\phi, t)$ with

$$\frac{1}{2} \sum_{\substack{\mathbf{y} \in \mathbb{Z}^n \cap t[-1,1]^n \\ \gcd(y_0, \ldots, y_{n-1}) = 1 \\ f_1(\mathbf{y}) \neq 0, f_2(\mathbf{y}) = 0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) + O(t^{n-2d}).$$

Using Möbius inversion and letting $\mathbf{y} = l\mathbf{x}$ we see that the sum over $\mathbf{y}$ equals

$$\sum_{\substack{\mathbf{y}\in\mathbb{Z}^n\cap t[-1,1]^n\\ f_1(\mathbf{y})\neq 0, f_2(\mathbf{y})=0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) \sum_{\substack{l\in\mathbb{Z}_{>0}\\ l|\mathbf{y}}} \mu(l) = \sum_{l\leq t}\mu(l) \sum_{\substack{\mathbf{x}\in\mathbb{Z}^n\cap \frac{t}{l}[-1,1]^n\\ f_1(\mathbf{x})\neq 0, f_2(\mathbf{x})=0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{x})),$$

because $\vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) = \vartheta_{\mathbb{Q}}(f_1(\mathbf{x}))$ holds due to $\deg(f_1)$ being even. Hence we have

$$N(\phi, t) = \frac{1}{2}\sum_{l\in\mathbb{Z}\cap[1,t]} \mu(l)\Theta_{\mathbb{Q}}(t/l) + O(t^{n-2d}),$$

and now the use of (3.1) and Lemma 1.3.36 for $R = 1$ yields

$$|\Theta_{\mathbb{Q}}(t)| \leq \#\{\mathbf{y}\in\mathbb{Z}^n\cap t[-1,1]^n : f_2(\mathbf{y}) = 0\} \ll t^{n-d},$$

which shows that the collective contribution from large l is

$$\begin{aligned}\Big|\sum_{l\in\mathbb{Z}_{>0}\cap(\log t, t]} \mu(l)\Theta_{\mathbb{Q}}(t/l)\Big| &\ll \sum_{l>\log t}(t/l)^{n-d} \ll t^{n-d}\sum_{l>\log t} l^{-2}\\ &\ll t^{n-d}(\log t)^{-1},\end{aligned}$$

where we used that $n - d \geq 2$ holds due to (3.1). □

For $m < 0$ the curve $x_0^2 + x_1^2 = mx_2^2$ has no $\mathbb{R}$-point, and therefore no $\mathbb{Q}$-point, in other words: $\vartheta_{\mathbb{Q}}(m) = 0$. Thus, writing $\max\{f_1([-1,1]^n)\}$ for $\max\{f_1(\mathbf{t}) : \mathbf{t}\in[-1,1]^n\}$, it is evident that we have the equality

$$\Theta_{\mathbb{Q}}(P) = \sum_{\substack{m\in\mathbb{Z}_{>0}\\ m\leq\max\{f_1([-1,1]^n)\}P^d}} \vartheta_{\mathbb{Q}}(m) \sum_{\substack{\mathbf{x}\in\mathbb{Z}^n\cap P[-1,1]^n\\ f_1(\mathbf{x})=m, f_2(\mathbf{x})=0}} 1.$$

Writing $\mathrm{d}\boldsymbol{\alpha}$ for $\mathrm{d}\alpha_1\mathrm{d}\alpha_2$ and using the identity

$$\int_{\boldsymbol{\alpha}\in[0,1)^2} \mathrm{e}(\alpha_1(f_1(\mathbf{x})-m)+\alpha_2 f_2(\mathbf{x}))\mathrm{d}\boldsymbol{\alpha} = \begin{cases}1, & \text{if } f_1(\mathbf{x}) = m \text{ and } f_2(\mathbf{x}) = 0,\\ 0, & \text{otherwise,}\end{cases}$$

shows the validity of

$$\Theta_{\mathbb{Q}}(P) = \int_{\boldsymbol{\alpha}\in[0,1)^2} S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\mathrm{d}\boldsymbol{\alpha}, \tag{3.10}$$

where one uses the notation

$$S(\boldsymbol{\alpha}) := \sum_{\mathbf{x}\in\mathbb{Z}^n\cap P[-1,1]^n} \mathrm{e}(\alpha_1 f_1(\mathbf{x}) + \alpha_2 f_2(\mathbf{x})) \tag{3.11}$$

and

$$E_{\mathbb{Q}}(\alpha_1) := \sum_{\substack{m\in\mathbb{Z}_{>0}\\ m\leq \max\{f_1([-1,1]^n)\}P^d}} \vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(\alpha_1 m) \tag{3.12}$$

to match the notation in Birch's work as outlined in §1.3.3. One has the obvious bound $E_{\mathbb{Q}}(\alpha_1) \ll P^d$ from the triangle inequality.

Recall the notation from Definition 1.3.24. We pick small positive θ_0 and δ as in (1.7) and (1.8), that is, such that we have $1 > \delta + 16\theta_0$ and $\frac{n-\sigma}{2^d} - 3(d-1) > \delta\theta_0^{-1}$. By the triangle inequality we have

$$\int_{\boldsymbol{\alpha}\notin\mathcal{M}(\theta_0)} \big|S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\big|\mathrm{d}\boldsymbol{\alpha} \leq \Big(\int_{\boldsymbol{\alpha}\notin\mathcal{M}(\theta_0)} |S(\boldsymbol{\alpha})|\mathrm{d}\boldsymbol{\alpha}\Big) \max_{\alpha_1\in[0,1)} |E_{\mathbb{Q}}(\alpha_1)|,$$

hence applying the result of Lemma 1.3.27 on the first factor, and using the trivial bound $E_{\mathbb{Q}}(\alpha_1) \ll P^d$ leads to the following bound on the integral away from $\mathcal{M}(\theta_0)$:

$$\int_{\boldsymbol{\alpha}\notin\mathcal{M}(\theta_0)} \big|S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\big|\mathrm{d}\boldsymbol{\alpha} \ll P^{n-d-\delta}.$$

By (3.10) this shows

$$\Theta_{\mathbb{Q}}(P) = \int_{\boldsymbol{\alpha}\in\mathcal{M}(\theta_0)} S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\mathrm{d}\boldsymbol{\alpha} + O(P^{n-d-\delta}).$$

Consistently modifying the setup, the following lemma is analogous to Lemma 1.3.29 and its proof is the same, using the notation introduced above. The essence of the lemma is the statement that in the expression for $\Theta_{\mathbb{Q}}(P)$ above, we may slightly modify the intervals of integration such that they are still disjoint.

LEMMA 3.2.2. *For any θ_0, δ satisfying* (1.7) *and* (1.8) *and under the assumptions of Theorem 3.1.3 we have*

$$\Theta_{\mathbb{Q}}(P) = \sum_{q\leq P^{2(d-1)\theta_0}} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \int_{\mathcal{M}'_{\mathbf{a},q}(\theta_0)} S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\mathrm{d}\boldsymbol{\alpha} + O(P^{n-d-\delta}),$$

where the modified set $\mathcal{M}'_{\mathbf{a},q}(\theta_0)$ consists of those $\boldsymbol{\alpha}\in[0,1]^2$ satisfying $|q\alpha_i - a_i| \leq qP^{-d+2(d-1)\theta_0}$.

Proof. Every modified interval $\mathcal{M}'_{\mathbf{a},q}(\theta_0)$ extends the associated interval $\mathcal{M}_{\mathbf{a},q}(\theta_0)$, so the estimate of the integral away from these intervals remains valid. One should only check that the modified intervals do not overlap. □

For $\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2$, write

$$S_{\mathbf{a},q} := \sum_{\mathbf{x} \in (\mathbb{Z} \cap [0,q))^n} \mathrm{e}\Big(\frac{a_1 f_1(\mathbf{x}) + a_2 f_2(\mathbf{x})}{q}\Big), \tag{3.13}$$

and for $\mathbf{\Gamma} \in \mathbb{R}^2$ define

$$I(\mathbf{\Gamma}) := \int_{\boldsymbol{\zeta} \in [-1,1]^n} \mathrm{e}(\Gamma_1 f_1(\boldsymbol{\zeta}) + \Gamma_2 f_2(\boldsymbol{\zeta}))\mathrm{d}\boldsymbol{\zeta}. \tag{3.14}$$

Recalling the notation $\eta = 2(d-1)\theta_0$, we now employ Lemma 1.3.32 with $\boldsymbol{\nu} = 0$ to evaluate $S(\alpha)$ and to see that under the assumptions of Lemma 3.2.2, with $\boldsymbol{\beta} := \boldsymbol{\alpha} - \mathbf{a}/q$, we have

$$\begin{aligned}\Theta_{\mathbb{Q}}(P) - P^n \sum_{q \le P^{2(d-1)\theta_0}} q^{-n} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} \int_{|\boldsymbol{\beta}| \le P^{-d+\eta}} I(P^d\boldsymbol{\beta})\overline{E_{\mathbb{Q}}(\beta_1 + a_1/q)}\mathrm{d}\boldsymbol{\beta} \\ \ll P^{n-d-\delta} + P^{n-1+2\eta} \sum_{q \le P^\eta} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} \int_{|\boldsymbol{\beta}| \le P^{-d+\eta}} |E_{\mathbb{Q}}(\beta_1 + a_1/q)|\mathrm{d}\boldsymbol{\beta}.\end{aligned}$$

By using $E_{\mathbb{Q}}(\alpha) \ll P^d$ once more we infer that the sum over q in the error term above is

$$\ll \sum_{q \le P^\eta} q^2 P^{2(-d+\eta)} P^d \ll P^{-d+5\eta},$$

hence we have proved the following lemma.

LEMMA 3.2.3. *Under the assumptions of Lemma 3.2.2,* $\Theta_{\mathbb{Q}}(P)P^{-n+d}$ *is*

$$\sum_{q \le P^\eta} q^{-n} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} \int_{|\boldsymbol{\beta}| \le P^{-d+\eta}} P^d I(P^d\boldsymbol{\beta})\overline{E_{\mathbb{Q}}(\beta_1 + a_1/q)}\mathrm{d}\boldsymbol{\beta}$$

up to an error term that is $O(P^{-\delta} + P^{-1+7\eta})$.

Proof. The proof consists merely of the calculations above. □

3.3 Exponential sums with terms detecting the existence of rational points

In this section we write x for $\max\{f_1([-1,1]^n)\}P^d$. As made clear by Lemma 3.2.3, to verify Theorem 3.1.3 we will asymptotically estimate the expression

$$E_{\mathbb{Q}}\Big(\frac{a_1}{q}+\beta_1\Big)=\sum_{\substack{m\in\mathbb{Z}_{>0}\cap[1,x]\\ x_0^2+x_1^2=mx_2^2 \text{ has a } \mathbb{Q}\text{-point}}} \mathrm{e}\left(\left(\frac{a_1}{q}+\beta_1\right)m\right),$$

for integers a_1, q, $\beta_1 \in \mathbb{R}$, and $x \in \mathbb{R}_{\geq 1}$. It suffices to first study the case $\beta_1 = 0$, and then to apply Lemma 3.3.7 at the end of this section. To study $E_{\mathbb{Q}}(a_1/q)$ we shall rephrase the condition on m in a way that it only regards the prime factorisation of m and then use the Rosser–Iwaniec sieve.

We begin by applying the formulas regarding Hilbert symbols in [Ser73, Ch.III,Th.1], which show that for strictly positive integers m one has

$$\vartheta_{\mathbb{Q}}(m)=\begin{cases}1, & \text{if } p\equiv 3 \,(\mathrm{mod}\ 4)\Rightarrow v_p(m)\equiv 0\,(\mathrm{mod}\ 2)\,,\\ 0, & \text{otherwise.}\end{cases} \tag{3.15}$$

Indeed, for $m \in \mathbb{Z}_{>0}$, the curve $x_0^2+x_1^2 = mx_2^2$ defines a smooth conic in $\mathbb{P}^2_{\mathbb{Q}}$ with an $\mathbb{R}$-point and the Hasse principle combined with Hilbert's product formula [Ser73, Ch.III,Th.3] proves (3.15). The function in (3.15) is the characteristic function of those integers m that are sums of two integral squares, see [Ten95, §4.8]. Landau [Ten95, Eq.(4.90)] proved the following asymptotic:

$$\sum_{1\leq m\leq x}\vartheta_{\mathbb{Q}}(m)=\frac{1}{2^{1/2}\mathcal{C}_0}\frac{x}{(\log x)^{1/2}}+O\bigg(\frac{x}{(\log x)^{3/2}}\bigg),\ x\in\mathbb{R}_{>1}, \tag{3.16}$$

but this is not sufficient for us since we will need a similar result restricted to those m in an arithmetic progression. Observe that the following holds

due to periodicity:

$$E_{\mathbb{Q}}\Big(\frac{a_1}{q}\Big) = \sum_{\substack{m\in\mathbb{Z}_{>0}\cap[1,x]\\ x_0^2+x_1^2=mx_2^2 \text{ has a } \mathbb{Q}\text{-point}}} \mathrm{e}\left(\frac{a_1}{q}m\right)$$
$$= \sum_{\ell\in\mathbb{Z}\cap[0,q)} \mathrm{e}(a_1\ell/q) \sum_{\substack{1\le m\le x\\ m\equiv\ell \pmod q}} \vartheta_{\mathbb{Q}}(m).$$

The work of Rieger [Rie65, Satz 1] could now be invoked to study the sum over $m \equiv \ell \pmod q$ when $\gcd(\ell, q) = 1$. One could attempt to use this to get asymptotic formulas for the cases with $\gcd(\ell, q) > 1$. However, we found it more straightforward to work instead with the function ϖ in place of $\vartheta_{\mathbb{Q}}$. This function $\varpi : \mathbb{Z}_{>0} \to \{0, 1\}$ is defined as

$$\varpi(m) := \begin{cases} 1, & \text{if } p \mid m \Rightarrow p \equiv 1 \pmod 4, \\ 0, & \text{otherwise.} \end{cases} \tag{3.17}$$

It is obvious that for all $m, k \in \mathbb{Z}_{>0}$ we have

$$\varpi(mk) = \varpi(m)\varpi(k) \tag{3.18}$$

so ϖ is completely multiplicative, while $\vartheta_{\mathbb{Q}}$ is merely multiplicative (to see this take $m = k = p$, where p is any prime which is $3 \pmod 4$). This is the reason for choosing to work with ϖ rather than $\vartheta_{\mathbb{Q}}$. Our next lemma shows how one can replace $\vartheta_{\mathbb{Q}}$ by ϖ, while simultaneously restricting the summation at the price of an error term.

LEMMA 3.3.1. *For $x, u \in \mathbb{R}_{\ge 1}$, $q \in \mathbb{Z}_{>0}$, $a_1 \in \mathbb{Z} \cap [0, q)$ we have*

$$\sum_{1\le m\le x} \vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q) = \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\ge 0}\\ 2^tk^2\le u\\ p\mid k\Rightarrow p\equiv 3 \pmod 4}} \sum_{\ell\in\mathbb{Z}\cap[0,q)} \mathrm{e}(a_1\ell/q) \sum_{\substack{r\in\mathbb{Z}_{>0}\\ 2^tk^2r\equiv\ell \pmod q\\ 1\le r\le x2^{-t}k^{-2}}} \varpi(r)$$

up to an error term that is $O\Big(\frac{x}{\sqrt{u}}\Big)$ with an absolute implied constant.

Proof. It is easy to see that for positive m one has $\vartheta_{\mathbb{Q}}(m) = 1$ if and only if we can write $m = 2^tk^2r$ for $t \in \mathbb{Z}_{\ge 0}$, k a positive integer all of whose

primes are $3 \pmod 4$ and r which satisfies $\varpi(r) = 1$. This shows that the sum over m is

$$\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3 (\mathrm{mod}\ 4)}} \sum_{\substack{r\in\mathbb{Z}_{>0}\\ 1\leq r\leq x2^{-t}k^{-2}}} \varpi(r)\,\mathrm{e}(a_1 2^t k^2 r/q).$$

The contribution of the pairs (k,t) with $2^t k^2 > u$ is at most

$$\sum_{t\geq 0}\sum_{k>\sqrt{u2^{-t}}} x2^{-t}k^{-2} < 2x\sum_{t\geq 0}\frac{2^{-t}}{\sqrt{u2^{-t}}} \ll \frac{x}{\sqrt{u}},$$

where the (first) inequality comes from Lemma 3.3.2.

Noting that $\mathrm{e}(a_1 2^t k^2 r/q)$ as a function of r is periodic modulo q allows to partition all r in congruences $\ell \in \mathbb{Z}/q\mathbb{Z}$, thus concluding the proof. □

Lemma 3.3.2. *For any $a \in \mathbb{R}_{>0}$ we have*

$$Z_a := \sum_{k\in\mathbb{Z}_{>a}} k^{-2} < 2a^{-1}.$$

Proof. For $a \geq 2$ we estimate the sum as a lower sum of the associated integral:

$$\sum_{k\in\mathbb{Z}_{>a}} k^{-2} \leq \int_{\lfloor a\rfloor}^{\infty} t^{-2}\mathrm{d}t = \lfloor a\rfloor^{-1}.$$

If a is an integer, then $\lfloor a\rfloor^{-1} < 2a^{-1}$ is obvious. If a is not an integer, then we have $\lfloor a\rfloor^{-1} = \lceil a-1\rceil^{-1} < (a-1)^{-1} < 2a^{-1}$ since a was at least 2.

We only still need to prove the statement for $a \in (0,2)$, for which we consider the sum separately. For $a \in (0,1)$ we have $Z_a = \zeta(2) < 2 < 2a^{-1}$ and for $a \in [1,2)$ we have $Z_a = \zeta(2) - 1 < 1 < 2a^{-1}$ again. □

The terms in the sum involving ϖ in Lemma 3.3.1 are in an arithmetic progression that is not necessarily primitive. We next show that we can reduce the evaluation of these sums to similar expressions where the summation is over an arithmetic progression that is primitive. The property (3.18) will be used for this.

LEMMA 3.3.3. *Let $t \in \mathbb{Z}_{\geq 0}$, $q \in \mathbb{Z}_{>0}$, $\ell \in \mathbb{Z} \cap [0, q)$ and $k \in \mathbb{Z}_{>0}$ be such that every prime divisor of k is $3 \pmod 4$. For $y \in \mathbb{R}_{>0}$ consider the sum*

$$\sum_{\substack{r \in \mathbb{Z}_{>0} \cap [1,y] \\ 2^t k^2 r \equiv \ell \pmod q}} \varpi(r).$$

The sum vanishes if $\gcd(2^t k^2, q) \nmid \ell$ holds, and it otherwise equals

$$\varpi\Big(\frac{\gcd(\ell, q)}{\gcd(2^t k^2, q)}\Big) \sum_{\substack{s \in \mathbb{Z}_{>0} \cap [1, y \gcd(2^t k^2, q) \gcd(\ell, q)^{-1}] \\ \frac{2^t k^2}{\gcd(2^t k^2, q)} s \equiv \frac{\ell}{\gcd(\ell, q)} \left(\mathrm{mod}\ \frac{q}{\gcd(\ell, q)}\right)}} \varpi(s).$$

Proof. If $\gcd(2^t k^2, q) \nmid \ell$ then the congruence $2^t k^2 r \equiv \ell \pmod q$ does not have a solution r, in which case the sum over r vanishes. On the other hand, if $\gcd(2^t k^2, q)$ divides ℓ, then we see that the congruence for r can be written equivalently as

$$\frac{2^t k^2}{\gcd(2^t k^2, q)} r \equiv \frac{\ell}{\gcd(2^t k^2, q)} \left(\mathrm{mod}\ \frac{q}{\gcd(2^t k^2, q)}\right).$$

Note that any solution r of this must necessarily satisfy

$$\gcd\Big(\frac{\ell}{\gcd(2^t k^2, q)}, \frac{q}{\gcd(2^t k^2, q)}\Big) \Big| \frac{2^t k^2}{\gcd(2^t k^2, q)} r,$$

the left-hand gcd being equal to $\gcd(\ell, q) \gcd(2^t k^2, q)^{-1}$. The fact of

$$\gcd\Big(\frac{\gcd(\ell, q)}{\gcd(2^t k^2, q)}, \frac{2^t k^2}{\gcd(2^t k^2, q)}\Big) = 1$$

shows that r must be divisible by $\gcd(\ell, q) \gcd(2^t k^2, q)^{-1}$. Therefore there exists an $s \in \mathbb{Z}_{>0}$ with

$$r = \frac{\gcd(\ell, q)}{\gcd(2^t k^2, q)} s$$

and substituting this into the sum over r in our lemma concludes the proof because

$$\varpi(r) = \varpi\Big(\frac{\gcd(\ell, q)}{\gcd(2^t k^2, q)}\Big) \varpi(s)$$

holds due to the complete multiplicativity seen in (3.18). □

We are now in a position to apply [FI10, Th.14.7], which is a result on the distribution of the function ϖ along primitive arithmetic progressions and which we include as a proposition for the convenience of the reader. We first introduce the following notation for $Q \in \mathbb{Z}_{>0}$:

$$\dot{Q} := \prod_{p \equiv 1 (\mathrm{mod}\ 4)} p^{v_p(Q)} \text{ and } \ddot{Q} := \prod_{p \equiv 3 (\mathrm{mod}\ 4)} p^{v_p(Q)}. \tag{3.19}$$

Proposition 3.3.4 ([FI10] Th.14.7). *Let Q be a positive integer multiple of 4, let $a \equiv 1 \,(\mathrm{mod}\ 4)$ satisfy $\gcd(a, Q) = 1$, and let z be any real number with $z \geq Q$. Then*

$$\sum_{\substack{r \in \mathbb{Z}_{>0} \cap [1,z] \\ r \equiv a (\mathrm{mod}\ Q)}} \varpi(r) = 2^{1/2} \mathcal{C}_0 \frac{\ddot{Q}}{\varphi(\ddot{Q})} \frac{z}{Q\sqrt{\log z}} \left\{ 1 + O\left(\left(\frac{\log Q}{\log z} \right)^{1/7} \right) \right\}$$

holds with an absolute implied constant.

Remark 3.3.5. This result is proven using the semi-linear Rosser–Iwaniec sieve. We should remark that there is a typo in the reference, namely[FI10, Eq.(14.22)] should instead read

$$V(D) = \prod_{2<p<D} \left(1 - \frac{1}{p}\right)^{\frac{1}{2}} \prod_{p<D} \left(1 - \frac{\chi(p)}{p}\right)^{-\frac{1}{2}} \prod_{\substack{2<p<D \\ p \equiv 3 (\mathrm{mod}\ 4)}} \left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}},$$

and as a result, [FI10, Eq.(14.39)] must be replaced by the asymptotic in Proposition 3.3.4. After fixing this typo, one can show, as in the proof of [FI10, Eq.(14.24)], that for $D \geq 2$, we have

$$\prod_{\substack{p<D \\ p \equiv 3 (\mathrm{mod}\ 4)}} \left(1 - \frac{1}{p}\right) = \frac{\sqrt{\pi}}{\sqrt{2}\exp(\gamma)} \mathcal{C}_0 \frac{1}{\sqrt{\log D}} + O\left(\frac{1}{(\log D)^{3/2}}\right). \tag{3.20}$$

There is a further typo in [FI10, Eq.(14.26)], namely, $c\sqrt{2}$ should be replaced by $2^{1/2}\mathcal{C}_0/4$.

We will now proceed to the application of Proposition 3.3.4. For any

$q \in \mathbb{Z}_{>0}, a_1 \in \mathbb{Z} \cap [0,q)$ define

$$\mathfrak{F}(a_1,q) := \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3 (\mathrm{mod}\ 4)}} \frac{\gcd(2^t k^2,q)}{2^t k^2} \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ \gcd(2^t k^2,q)|\ell \\ (3.22)}} \frac{\varpi\big(\frac{\gcd(\ell,q)}{\gcd(2^t k^2,q)}\big)\,\mathrm{e}\left(\frac{a_1\ell}{q}\right)}{\gcd(\ell,q)\mathrm{lcm}\big(4,\frac{q}{\gcd(\ell,q)}\big)} \times \prod_{\substack{p\equiv 3 (\mathrm{mod}\ 4)\\ v_p(q)>v_p(\ell)}} \Big(1-\frac{1}{p}\Big)^{-1}, \tag{3.21}$$

where ℓ in the summation satisfies

$$\frac{2^t k^2}{\gcd(2^t k^2,q)} \equiv \frac{\ell}{\gcd(\ell,q)} \left(\mathrm{mod}\ \gcd\Big(4,\frac{q}{\gcd(\ell,q)}\Big)\right). \tag{3.22}$$

The result of the following lemma aims to separate out the dependence on x from the apparent pandemonium that is hidden in $\mathfrak{F}(a_1,q)$.

Lemma 3.3.6. *For $x \in \mathbb{R}_{\geq 1}$, $A \in \mathbb{R}_{>0}, q \in \mathbb{Z}_{>0}, a_1 \in \mathbb{Z}\cap[0,q)$ with $q \leq (\log x)^A$ we have*

$$\sum_{\substack{m\in\mathbb{Z}\cap[1,x]\\ x_0^2+x_1^2=mx_2^2 \text{ has}\\ a\ \mathbb{Q}\text{-point}}} \mathrm{e}\left(a_1\frac{m}{q}\right) = 2^{1/2}\mathcal{C}_0\mathfrak{F}(a_1,q)\frac{x}{(\log x)^{1/2}} + O_A\left(\frac{q^3 x}{(\log x)^{1/2+1/7}}\right),$$

where the implied constant depends at most on A.

Proof. Combining Lemma 3.3.1 with $u = (\log x)^{100}$ and Lemma 3.3.3 shows that, up to an error term which is $\ll x(\log x)^{-50}$, the sum over m in our lemma equals

$$\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^t k^2\leq(\log x)^{100}\\ p|k\Rightarrow p\equiv 3(\mathrm{mod}\ 4)}} \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ \gcd(2^t k^2,q)|\ell}} \varpi\Big(\frac{\gcd(\ell,q)}{\gcd(2^t k^2,q)}\Big)\,\mathrm{e}(a_1\ell/q) \times \sum_{\substack{s\in\mathbb{Z}_{>0}\cap[1,x2^{-t}k^{-2}\gcd(2^t k^2,q)\gcd(\ell,q)^{-1}]\\ \frac{2^t k^2}{\gcd(2^t k^2,q)}s\equiv\frac{\ell}{\gcd(\ell,q)}\left(\mathrm{mod}\ \frac{q}{\gcd(\ell,q)}\right)}} \varpi(s).$$

We note that $\varpi(s)$ vanishes unless s satisfies $s \equiv 1 \,(\mathrm{mod}\ 4)$. This means that we can add the condition $s \equiv 1 \,(\mathrm{mod}\ 4)$ in the last sum over s, thus

resulting with the double congruence

$$s \equiv 1 \,(\mathrm{mod}\ 4)\,, \frac{2^t k^2}{\gcd(2^t k^2, q)} s \equiv \frac{\ell}{\gcd(\ell, q)} \left(\mathrm{mod}\ \frac{q}{\gcd(\ell, q)}\right).$$

By the Chinese remainder theorem this has a solution if and only if (3.22) is satisfied. Assuming that this happens, the solution is unique modulo

$$Q := \mathrm{lcm}\Big(4, \frac{q}{\gcd(\ell, q)}\Big).$$

Hence by Proposition 3.3.4 we get that the sum over m in our lemma equals

$$\begin{aligned}\mathrm{MT} :&= 2^{1/2}\mathcal{C}_0 \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^t k^2 \leq (\log x)^{100}\\ p|k \Rightarrow p\equiv 3 (\mathrm{mod}\ 4)}} \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q),(3.22)\\ \gcd(2^t k^2, q)|\ell}} \varpi\Big(\frac{\gcd(\ell,q)}{\gcd(2^t k^2, q)}\Big)\, \mathrm{e}(a_1\ell/q)\\ &\times \frac{\ddot{Q}}{\varphi(\ddot{Q})} \frac{1}{\mathrm{lcm}(4, q/\gcd(\ell,q))} \frac{x 2^{-t} k^{-2} \gcd(2^t k^2, q)\gcd(\ell,q)^{-1}}{\sqrt{\log(x 2^{-t} k^{-2}\gcd(2^t k^2, q)\gcd(\ell,q)^{-1})}}\end{aligned}$$

up to an error term which is

$$\begin{aligned}&\ll \frac{x}{(\log x)^{50}} \qquad (3.23)\\ &+ \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^t k^2 \leq (\log x)^{100}\\ p|k\Rightarrow p\equiv 3(\mathrm{mod}\ 4)}} \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ \gcd(2^t k^2,q)|\ell\\ (3.22)}} (\log\log\ddot{Q}) \frac{x 2^{-t}k^{-2}\gcd(2^t k^2, q)}{\gcd(\ell,q)\sqrt{\log x}} \Big(\frac{\log Q}{\log x}\Big)^{1/7}\end{aligned}$$

owing to (3.5), which gives $\ddot{Q}/\varphi(\ddot{Q}) \ll \log\log\ddot{Q} \leq \log\log Q$, combined with the trivial bounds $\varpi(\cdot), \mathrm{e}(a_1\ell/q), Q^{-1} \leq 1$. Note that we have made use of

$$\log(x 2^{-t} k^{-2}\gcd(2^t k^2, q)\gcd(\ell,q)^{-1}) = \log x + O_A(\log\log x), \qquad (3.24)$$

which follows from

$$\frac{x}{(\log x)^{100+A}} \leq \frac{x}{2^t k^2 q} \leq x 2^{-t} k^{-2} \frac{\gcd(2^t k^2, q)}{\gcd(\ell, q)} \leq xq \leq x(\log x)^A.$$

The bound $\ddot{Q} \le Q \le 4q$ shows that the sum over t, k in (3.23) is

$$\begin{aligned}
&\ll (\log\log q)(\log q)^{1/7} \frac{x}{(\log x)^{1/2+1/7}} \sum_{(k,t)} \sum_{\ell \in \mathbb{Z} \cap [0,q)} 2^{-t} k^{-2} \gcd(2^t k^2, q) \\
&\ll (\log\log q)(\log q)^{1/7} \frac{x}{(\log x)^{1/2+1/7}} q^2 \sum_{(k,t) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\ge 0}} 2^{-t} k^{-2} \\
&\ll q^3 \frac{x}{(\log x)^{1/2+1/7}},
\end{aligned}$$

which is satisfactory. To conclude the proof, it remains to show that the quantity MT gives rise to the main term as stated in our lemma. By (3.24) we see that

$$\frac{1}{\sqrt{\log(x 2^{-t} k^{-2} \gcd(2^t k^2, q) \gcd(\ell, q)^{-1})}} = \frac{1}{\sqrt{\log x}} + O\Big(\frac{\log\log x}{(\log x)^{3/2}}\Big),$$

hence $\mathrm{MT} = \mathrm{M}' + \mathrm{R}$, where M' is defined by

$$\begin{aligned}
&\frac{x 2^{1/2} \mathcal{C}_0}{(\log x)^{1/2}} \sum_{\substack{(k,t) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\ge 0} \\ 2^t k^2 \le (\log x)^{100} \\ p \mid k \Rightarrow p \equiv 3 \pmod 4}} \frac{\gcd(2^t k^2, q)}{2^t k^2} \\
&\qquad \times \sum_{\substack{\ell \in \mathbb{Z} \cap [0,q) \\ \gcd(2^t k^2, q) \mid \ell \\ (3.22)}} \frac{\varpi(\gcd(\ell, q)/\gcd(2^t k^2, q)) \, \mathrm{e}(a_1 \ell / q) \ddot{Q}}{\gcd(\ell, q) \mathrm{lcm}(4, q/\gcd(\ell, q)) \varphi(\ddot{Q})}
\end{aligned}$$

and R is a quantity that satisfies

$$\mathrm{R} \ll \sum_{(k,t) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\ge 0}} \sum_{\ell \in \mathbb{Z} \cap [0,q)} \frac{\ddot{Q}}{\varphi(\ddot{Q})} \frac{x 2^{-t} k^{-2} \gcd(2^t k^2, q)}{(\log\log x)^{-1} (\log x)^{3/2}} \ll q^3 \frac{x \log\log x}{(\log x)^{3/2}},$$

where we again have made use of the trivial upper bound 1 for $\varpi(\cdot)$ and $|\mathrm{e}(\cdot)|$, now combined with the lower bound 1 for $\mathrm{lcm}(\cdot)$ and $\gcd(\cdot)$. The cubic power of q arises from bounding both $\gcd(2^t k^2, q)$ and $\ddot{Q}/\varphi(\ddot{Q})$ from above by q, and then having q terms in the sum $\sum_{\ell \in \mathbb{Z} \cap [0,q)} 1$. As we have seen before, we could have bounded $\ddot{Q}/\varphi(\ddot{Q})$ from above by $\log\log q$, but this extra saving is unnecessary for our goals.

We complete the summation over t, k in M' to the whole range $\mathbb{Z}_{>0} \times \mathbb{Z}_{\ge 0}$

appearing in (3.21). To do so, we use the bound

$$\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^tk^2>(\log x)^{100}}}\frac{\gcd(2^tk^2,q)}{2^tk^2}\sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ (3.22)\\ \gcd(2^tk^2,q)|\ell}}\frac{\ddot{Q}}{\varphi(\ddot{Q})}\ll q^3\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^tk^2>(\log x)^{100}}}\frac{1}{2^tk^2}\ll\frac{q^3}{(\log x)^{50}},$$

while the observation

$$\frac{\ddot{Q}}{\varphi(\ddot{Q})}=\prod_{\substack{p\equiv 3(\mathrm{mod}\ 4)\\ p|q(\gcd(\ell,q))^{-1}}}\Big(1-\frac{1}{p}\Big)^{-1}=\prod_{\substack{p\equiv 3(\mathrm{mod}\ 4)\\ v_p(q)>v_p(\ell)}}\Big(1-\frac{1}{p}\Big)^{-1}$$

allows to remove $\ddot{Q}$ from M′. □

We note that one immediate corollary of the last lemma is the bound

$$\mathfrak{F}(a_1,q)\ll 1, \tag{3.25}$$

with an absolute implied constant. Indeed, this can be shown by taking $A=1/100$ in Lemma 3.3.6, dividing throughout by $x/\sqrt{\log x}$ in the asymptotic it provides and applying (3.16) to obtain

$$\begin{aligned}2^{1/2}\mathcal{C}_0\mathfrak{F}(a_1,q)&\ll\frac{(\log x)^{1/2}}{x}\Big|\sum_{1\leq m\leq x}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q)\Big|+\frac{q^3}{(\log x)^{1/7}}\\&\ll 1+\frac{(\log x)^{3/100}}{(\log x)^{1/7}}.\end{aligned}$$

We remark that although this argument may feel somewhat circular at first glance, it is in fact not since the second estimate in the above equality follows not from the lemma, but from the triangle inequality combined with (3.16).

As announced at the beginning of this section, studying $E_{\mathbb{Q}}\Big(\frac{a_1}{q}+\beta_1\Big)$ is first done in the case $\beta_1=0$ as in Lemma 3.3.6 with $x=\max\{f([-1,1]^n)\}P^d$. The following lemma shows that this is sufficient, up to introducing an extra factor.

Lemma 3.3.7. *For $\Gamma_1\in\mathbb{R}$, $A\in\mathbb{R}_{>0}$, $q\in\mathbb{Z}_{>0}$ with $q\leq(\log P)^A$, and $a_1\in\mathbb{Z}\cap[0,q)$ we have*

$$E_{\mathbb{Q}}\bigg(\frac{a_1}{q}+\frac{\Gamma_1}{P^d}\bigg)=2^{1/2}\mathcal{C}_0\mathfrak{F}(a_1,q)\bigg(\int_2^{\max\{f_1([-1,1]^n)\}P^d}\frac{\mathrm{e}(\Gamma_1P^{-d}t)}{\sqrt{\log t}}\mathrm{d}t\bigg)$$

up to an error term that is $O_A\Big(\frac{q^3(1+|\Gamma_1|)P^d}{(\log P)^{1/2+1/7}}\Big)$.

Proof. To ease the notation we temporarily put $c := 2^{1/2}\mathcal{C}_0\mathfrak{F}(a_1,q)$. Fix $\beta\in\mathbb{R}$. By applying partial summation[1] with $a_m = \vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q))$ and $\varphi(t)=\mathrm{e}(\beta t)$, we see that $\sum_{m\le x}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(m(\beta+a_1/q))$ equals

$$\Big(\sum_{m\le x}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q)\Big)\,\mathrm{e}(x\beta)-\int_0^x \mathrm{e}(\beta t)'\Big(\sum_{m\le t}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q)\Big)\mathrm{d}t.$$

For $q\le(\log x)^A$, Lemma 3.3.6 shows that this equals

$$c\Big(\Big(\frac{x}{\sqrt{\log x}}\,\mathrm{e}(x\beta)-\int_2^x\frac{t}{\sqrt{\log t}}\,\mathrm{e}(\beta t)'\mathrm{d}t\Big)+O_A\Big(\frac{q^3x(1+|\beta|x)}{(\log x)^{1/2+1/7}}\Big),$$

with an implied constant depending at most on A. Using partial integration this is plainly

$$c\Big(\int_2^x\Big(\frac{t}{\sqrt{\log t}}\Big)'\,\mathrm{e}(\beta t)\mathrm{d}t\Big)+O_A\Big(\frac{q^3(1+|\beta|x)x}{(\log x)^{1/2+1/7}}\Big),$$

and using $(t(\log t)^{-1/2})' = (\log t)^{-1/2}-2^{-1}(\log t)^{-3/2}$ shows that the last integral can be evaluated as $\int_2^x\mathrm{e}(\beta t)(\log t)^{-1/2}\mathrm{d}t+O(x(\log x)^{-3/2})$. Invoking the bound $c\ll 1$ (that is implied by (3.25)) we obtain

$$\sum_{m\le x}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(m(\beta+a_1/q))=c\Big(\int_2^x\frac{\mathrm{e}(\beta t)}{\sqrt{\log t}}\mathrm{d}t\Big)+O\Big(\frac{q^3(1+|\beta|x)x}{(\log x)^{1/2+1/7}}\Big).$$

Using this for $x=\frac12\min\{f_1([-1,1]^n)\}P^d$ and putting $\beta=\Gamma_1P^{-d}$ concludes the proof. □

3.4 Proof of the asymptotic

We are ready to prove the asymptotic in Theorem 3.1.3. We shall do so with different leading constants than those given in Theorem 3.1.3; showing equality of the constants is delayed until §3.5.

[1] See Theorem 1.3.1.

3.4.1 Restricting the range in the major arcs

The first reasonable step for the proof of the asymptotics would be to inject Lemma 3.3.7 into Lemma 3.2.3. However, this would give poor results because the error term in Lemma 3.3.7 is only powerful when Γ_1 is close to zero and q is small in comparison to P. For this reason we restrict the sum over q and the integration over $\boldsymbol{\beta}$ in Lemma 3.2.3. For its proof we shall need certain bounds. First, by (3.16) and the triangle inequality, one has

$$E_{\mathbb{Q}}(\alpha_1) \ll P^d(\log P)^{-1/2} \tag{3.26}$$

where the implied constant is independent of α_1. Recall the definition of $I(\mathbf{\Gamma})$ from (3.14). Letting $K := (n-\sigma(f_1,f_2))2^{-d+1}$, we use Lemmas 1.3.33 and 1.3.34 to obtain the following bounds valid for every $\varepsilon > 0$, $\mathbf{\Gamma} \in \mathbb{R}^2$ and $\mathbf{a} \in \mathbb{Z}^2, q \in \mathbb{Z}_{>0}$ satisfying $\gcd(a_1,a_2,q)=1$:

$$I(\mathbf{\Gamma}) \ll_\varepsilon \min\{1, |\mathbf{\Gamma}|^{-K/(2(d-1))+\varepsilon}\} \text{ and } S_{\mathbf{a},q} \ll_\varepsilon q^{n-K/(2(d-1))+\varepsilon}.$$

By our assumption (3.1), we have

$$I(\mathbf{\Gamma}) \ll \min\{1, |\mathbf{\Gamma}|^{-5/2}\}, \tag{3.27}$$

and furthermore, for all $0 < \lambda < 2^{-d}(d-1)^{-1}$ we have

$$S_{\mathbf{a},q} \ll_\lambda q^{n-3-\lambda}. \tag{3.28}$$

Lemma 3.4.1. *Keep the assumptions of Lemma 3.2.2 and let $Q_1, Q_2 \in \mathbb{R}_{\geq 1}$ with $Q_1, Q_2 \leq P^\eta$ for some fixed positive η. Then for any λ satisfying*

$$0 < \lambda < \min\Big\{1, \frac{1}{2}\Big(\frac{n-\sigma(f_1,f_2)}{2^d(d-1)} - 3\Big)\Big\} \tag{3.29}$$

we have

$$\begin{aligned}
&\sum_{q \leq P^\eta} q^{-n} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} \int_{|\boldsymbol{\beta}| \leq P^{-d+\eta}} P^d I(P^d\boldsymbol{\beta}) \overline{E_{\mathbb{Q}}(\beta_1 + a_1/q)} \mathrm{d}\boldsymbol{\beta} \\
&= \sum_{q \leq Q_1} q^{-n} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} \int_{|\mathbf{\Gamma}| \leq Q_2} \frac{I(\mathbf{\Gamma})}{P^d} \overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d} + a_1/q)} \mathrm{d}\mathbf{\Gamma} \\
&+ O_{\delta,\lambda,\theta_0}\big((\log P)^{-1/2} \min\big\{Q_1^{-\lambda}, Q_2^{-1/2}\big\}\big).
\end{aligned}$$

Proof. Using the change of variables $P^d\boldsymbol{\beta} = \boldsymbol{\Gamma}$ we obtain equality between

$$\int_{P^{-d}Q_2<|\boldsymbol{\beta}|\leq P^{-d+\eta}} P^d I(P^d\boldsymbol{\beta})\overline{E_{\mathbb{Q}}(\beta_1+a_1/q)}\mathrm{d}\boldsymbol{\beta}$$

and

$$P^{-d}\int_{Q_2<|\boldsymbol{\Gamma}|\leq P^{\eta}} I(\boldsymbol{\Gamma})\overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d}+a_1/q)}\mathrm{d}\boldsymbol{\Gamma}.$$

We bound $\overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d}+a_1/q)}$ by $P^d(\log P)^{-1/2}$ from (3.26), where the implied constant did not depend on the argument of $E_{\mathbb{Q}}$. We bound $I(\boldsymbol{\Gamma})$ using (3.27), and we extend the range of integration to $Q_2 < |\boldsymbol{\Gamma}|$.

The bound $\int_{Q_2<|\boldsymbol{\Gamma}|} I(\boldsymbol{\Gamma})\mathrm{d}\boldsymbol{\Gamma} \ll Q_2^{-1/2}$ may be computed in a straightforward manner using (3.27) and dividing up the range of integration to make use of the symmetry of the problem. These estimates together show the validity of

$$\int_{P^{-d}Q_2<|\boldsymbol{\beta}|\leq P^{-d+\eta}} P^d I(P^d\boldsymbol{\beta})\overline{E_{\mathbb{Q}}(\beta_1+a_1/q)}\mathrm{d}\boldsymbol{\beta} \ll \frac{1}{\sqrt{Q_2\log P}}. \tag{3.30}$$

This shows that the sum over $q \leq P^{\eta}$ in the statement of our lemma equals

$$\sum_{q\leq P^{\eta}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q}\int_{|\boldsymbol{\Gamma}|\leq Q_2} \frac{I(\boldsymbol{\Gamma})}{P^d}\overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d}+a_1/q)}\mathrm{d}\boldsymbol{\Gamma}$$

up to a term that is

$$\ll \frac{1}{\sqrt{Q_2\log P}}\sum_{q\leq P^{\eta}}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{|S_{\mathbf{a},q}|}{q^n} \ll \frac{\sum_{q\leq P^{\eta}} q^{-1-\lambda}}{\sqrt{Q_2\log P}} \ll \frac{1}{\sqrt{Q_2\log P}},$$

where (3.28) has been utilised. Note that the bound $\int_{\mathbb{R}^2}|I(\boldsymbol{\Gamma})|\mathrm{d}\boldsymbol{\Gamma} < \infty$ is a consequence of (3.27). Using this with (3.26) shows

$$\sum_{q>Q_1}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{S_{\mathbf{a},q}}{q^n}\int_{|\boldsymbol{\Gamma}|\leq Q_2} I(\boldsymbol{\Gamma})\overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d}+a_1/q)}\mathrm{d}\boldsymbol{\Gamma} \ll \frac{\sum_{q>Q_1} q^{-1-\lambda}}{\sqrt{\log P}}$$
$$\ll \frac{Q_1^{-\lambda}}{\sqrt{\log P}},$$

where we have used (3.28). This concludes the proof of the lemma. □

LEMMA 3.4.2. *Keep the assumptions of Lemma 3.2.2, fix any two positive A_1, A_2, and let*

$$\lambda_0 := \frac{1}{2}\min\left\{1, \frac{1}{2}\left(\frac{n-\sigma(f_1,f_2)}{2^d(d-1)} - 3\right)\right\}. \tag{3.31}$$

Then for all sufficiently large P the quantity $\Theta_{\mathbb{Q}}(P)P^{-n+d}$ equals

$$\sum_{q\le(\log P)^{A_1}} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{S_{\mathbf{a},q}}{q^n} \int_{|\mathbf{\Gamma}|\le(\log P)^{A_2}} \frac{I(\mathbf{\Gamma})}{P^d}\overline{E_{\mathbb{Q}}\left(\frac{a_1}{q}+\frac{\Gamma_1}{P^d}\right)}\mathrm{d}\mathbf{\Gamma}$$

up to an error term that is $O_{A_1,A_2}\big((\log P)^{-1/2-\min\{A_1\lambda_0,A_2/2\}}\big)$.

Proof. The proof follows immediately from application of Lemma 3.4.1 with $Q_i = (\log P)^{A_i}$ and Lemma 3.2.3 with some fixed δ and θ_0 satisfying (1.7) and (1.8) and subject to $\eta = 2(d-1)\theta_0 < 1/7$ in order to get a negative power of P in the error term coming from Lemma 3.4.1. □

3.4.2 Injecting the sieve estimates into the restricted major arcs

We are now in a position to inject Lemma 3.3.7 into Lemma 3.4.2. It may be uncommon to use sieve estimates to study major arcs, but the reason that we do this is not very deep: the availability of the sieve estimates allowed us to not worry about the behaviour of $\vartheta_{\mathbb{Q}}(m)$ in residue classes. It is not at all unlikely that good results on $\vartheta_{\mathbb{Q}}(m)$ in residue classes allow for a much more direct approach.

It will be convenient to start by studying the archimedean density, but before we do all that, we state a basic lemma that will be used twice in this chapter.

LEMMA 3.4.3. *For $x \ge 2$ we have*

$$\int_2^x (\log t)^{-1/2}\mathrm{d}t \ll \frac{x}{\sqrt{\log x}}.$$

Proof. Note that $\frac{t}{\sqrt{\log t}}$ is the anti-derivative of $\frac{2\log t-1}{2(\log t)^{3/2}}$ and that we have

$$(\log t)^{-1/2} \ll \frac{2\log t - 1}{2(\log t)^{3/2}}.$$

Hence we get

$$\int_2^x (\log t)^{-1/2}\mathrm{d}t \ll \frac{x}{\sqrt{\log x}}.$$

□

Now recall (3.14) and define for all P with $2 \le \max\{f_1([-1,1]^n)\}P^d$ the integral

$$\mathfrak{J}_\phi(P) := \int_{\mathbf{\Gamma}\in\mathbb{R}^2} \frac{I(\mathbf{\Gamma})}{P^d}\bigg(\int_2^{\max\{f_1([-1,1]^n)\}P^d} \frac{\mathrm{e}(-\Gamma_1 P^{-d}t)}{\sqrt{\log t}}\mathrm{d}t\bigg)\mathrm{d}\mathbf{\Gamma}. \quad (3.32)$$

The assumptions of Theorem 3.1.3 ensure that the integral converges absolutely, since by (3.27) and application of Lemma 3.4.3 we have

$$\begin{aligned}\int_{\mathbf{\Gamma}\in\mathbb{R}^2} \frac{|I(\mathbf{\Gamma})|}{P^d}\int_2^{\max\{f_1([-1,1]^n)\}P^d} \frac{\mathrm{d}t\mathrm{d}\mathbf{\Gamma}}{\sqrt{\log t}} &\ll \int_{\mathbf{\Gamma}\in\mathbb{R}^2} \frac{\min\{1,|\mathbf{\Gamma}|^{-5/2}\}}{P^d}\frac{P^d\mathrm{d}\mathbf{\Gamma}}{\sqrt{\log P}}\\ &\ll \frac{1}{\sqrt{\log P}}.\end{aligned}$$

Lemma 3.4.4. *Under the assumptions of Theorem 3.1.3 we have*

$$\mathfrak{J}_\phi(P) = \frac{1}{\sqrt{\log(P^d)}}\int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma})\bigg(\int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu)\mathrm{d}\mu\bigg)\mathrm{d}\mathbf{\Gamma}$$

up to an error term that is $O((\log P)^{-3/2})$.

Proof. Observe that the change of variables $\mu = P^{-d}t$ in (3.32) shows

$$\mathfrak{J}_\phi(P) = \int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma})\bigg(\int_{2P^{-d}}^{\max\{f_1([-1,1]^n)\}} \frac{\mathrm{e}(-\Gamma_1\mu)}{\sqrt{\log(\mu P^d)}}\mathrm{d}\mu\bigg)\mathrm{d}\mathbf{\Gamma}.$$

For $|x| < 1$ we have $(1+x)^{-1/2} = 1 + O(x)$, hence for fixed μ we have

$$\begin{aligned}\big(\log(\mu P^d)\big)^{-1/2} &= \big(\log(P^d)\big)^{-1/2}\bigg(1+\frac{\log\mu}{\log(P^d)}\bigg)^{-1/2}\\ &= \big(\log(P^d)\big)^{-1/2} + O\bigg(\frac{\log\mu}{(\log P)^{3/2}}\bigg).\end{aligned}$$

Using this for $0 < \mu \le \max\{f_1([-1,1]^n)\}$, we infer the following estimate for all sufficiently large P, where the integral $\int_{2P^{-d}}^{\max\{f_1([-1,1]^n)\}}\log\mu\mathrm{d}\mu$ is bounded by a constant. The difference

$$\mathfrak{J}_\phi(P) - \frac{1}{\sqrt{\log(P^d)}}\int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma})\int_{2P^{-d}}^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu)\mathrm{d}\mu\mathrm{d}\mathbf{\Gamma}$$

can be estimated as

$$\ll \frac{1}{(\log P)^{3/2}} \int_{\mathbf{\Gamma}\in\mathbb{R}^2} |I(\mathbf{\Gamma})| \mathrm{d}\mathbf{\Gamma} \ll (\log P)^{-3/2}$$

due to (3.27). □

Define

$$\mathfrak{J} := \int_{\Gamma\in\mathbb{R}} \int_{\{\mathbf{t}\in[-1,1]^n : x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \text{ has an } \mathbb{R}\text{-point}\}} \mathrm{e}(\Gamma f_2(\mathbf{t})) \mathrm{d}\mathbf{t}\mathrm{d}\Gamma \tag{3.33}$$

and note that the integral converges absolutely owing to (3.1) and Lemma 1.3.33 with $R = 1$. The arguments in [Bir62, §6] show that if the set $\{\mathbf{t} \in [-1,1]^n : f_1(\mathbf{t}) \geq 0\}$ contains a non-singular real point of $f_2 = 0$ then $\mathfrak{J} > 0$. This condition holds in the situation of Theorem 3.1.3 because its assumptions include $B(\mathbb{Q}) \neq \emptyset$ and that f_2 is non-singular. This will again come up in the proof of Theorem 3.5.23, where we give more details.

Lemma 3.4.5. *Under the assumptions of Theorem 3.1.3 we have*

$$\int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma}) \bigg(\int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu) \mathrm{d}\mu \bigg) \mathrm{d}\mathbf{\Gamma} = \mathfrak{J}.$$

Proof. This proof will follow the same arguments as [DS18, Lem. 4.3 and 4.4]. First we will show that the left-hand side of the equation in the lemma is equal to $\lim_{m\to\infty} \mathfrak{J}_m$ with

$$\mathfrak{J}_m = \int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma}) \exp\left(-\pi^2\Gamma_1^2 m^{-2}\right) \int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu) \mathrm{d}\mu \mathrm{d}\mathbf{\Gamma}.$$

We consider

$$\begin{aligned}
&\left| \int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma}) \bigg(\int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu) \mathrm{d}\mu \bigg) \mathrm{d}\mathbf{\Gamma} - \mathfrak{J}_m \right| \\
&= \left| \int_{\Gamma_1\in\mathbb{R}} \big(1 - \exp(-\pi^2\Gamma_1^2 m^{-2}\big) \int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu) \mathrm{d}\mu \int_{\Gamma_2\in\mathbb{R}} I(\mathbf{\Gamma}) \mathrm{d}\Gamma_2 \mathrm{d}\Gamma_1 \right| \\
&\ll \left| \int_{\Gamma_1\in\mathbb{R}} \big(1 - \exp(-\pi^2\Gamma_1^2 m^{-2}\big) \int_{\Gamma_2\in\mathbb{R}} I(\mathbf{\Gamma}) \mathrm{d}\Gamma_2 \mathrm{d}\Gamma_1 \right|.
\end{aligned}$$

We split the integration range of Γ_1 into two parts: $|\Gamma_1| \leq \log m$ and $|\Gamma_1| > \log m$. Making use of (3.27) we estimate the first part of the integral as

$$O\left((1-\exp(-\pi^2 m^{-2}(\log m)^2))\log m\right),$$

which goes to 0 for $m \to \infty$.

For the second part, we bound $1-\exp(-\pi^2\Gamma_1^2 m^{-2})$ by 1, and again make use of (3.27) to conclude that the integral is $O\left((\log m)^{-1/2}\right)$, which goes to 0 for $m \to \infty$. Therefore, we have proven that the integral in the statement of the lemma is equal to the limit $\lim_{m\to\infty}\mathfrak{J}_m$. We continue with the proof that this limit also equals $\mathfrak{J}$.

Define for $m \in \mathbb{Z}_{>0}$ the function $\phi_m : \mathbb{R} \to \mathbb{R}$ by

$$\phi_m(x) := \pi^{-1/2} m \exp\left(-m^2x^2\right).$$

The Fourier transform of $\phi_m(x)$ is $\exp(-\pi^2\xi^2 m^{-2})$, hence by Fourier's inversion formula, we have

$$\phi_m(x) = \int_{\mathbb{R}} \exp\left(-\pi^2\Gamma_1^2 m^{-2}\right) \mathrm{e}(x\Gamma_1)\mathrm{d}\Gamma_1.$$

Using this with $x = f_1(\mathbf{t}) - \mu$, and inserting the definition of $I(\mathbf{\Gamma})$, allows us to rewrite $\mathfrak{J}_m$ as

$$\int_{\substack{\mathbf{t}\in[-1,1]^n : f_1(\mathbf{t})\neq 0 \\ f_1(\mathbf{t})\neq \max\{f_1([-1,1]^n)\}}} \left(\int_0^{\max\{f_1([-1,1]^n)\}} \phi_m(f_1(\mathbf{t})-\mu)\mathrm{d}\mu\right)\left(\int_{\Gamma_2\in\mathbb{R}} \mathrm{e}(\Gamma_2 f_2(\mathbf{t}))\mathrm{d}\Gamma_2\right)\mathrm{d}\mathbf{t}.$$

Note that we replaced $\mathbf{t} \in [-1,1]^n$ by the range of integration in the expression above; this is allowed as it only removes a set of measure zero from the integration in (3.14).

The following identity for real numbers $a < b$ and $a \neq c \neq b$ is well known and easily proven:

$$\lim_{m\to\infty}\int_a^b \phi_m(c-\mu)\mathrm{d}\mu = \begin{cases} 1 & \text{if } a < c < b, \\ 0 & \text{otherwise.} \end{cases}$$

Hence if $\mathbf{t} \in [-1,1]^n$ satisfies $f_1(\mathbf{t}) > 0$ and $f_1(\mathbf{t}) \neq \max\{f_1([-1,1]^n)\}$, then we have

$$\lim_{m\to\infty}\int_0^{\max\{f_1([-1,1]^n)\}} \phi_m(f_1(\mathbf{t})-\mu)\mathrm{d}\mu = 1,$$

while for $f_1(\mathbf{t}) < 0$ the limit vanishes. The dominated convergence theorem allows us to switch the order of the limit over m and the integral over $\mathbf{t}$, providing

$$\begin{aligned}\int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma}) \int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu)\mathrm{d}\mu\mathrm{d}\mathbf{\Gamma}&\\ = \int_{\substack{\mathbf{t}\in[-1,1]^n: f_1(\mathbf{t})>0\\ f_1(\mathbf{t})\neq\max\{f_1([-1,1]^n)\}}} \left(\int_{\Gamma_2\in\mathbb{R}} \mathrm{e}(\Gamma_2 f_2(\mathbf{t}))\mathrm{d}\Gamma_2\right)\mathrm{d}\mathbf{t}&\\ = \int_{\substack{\mathbf{t}\in[-1,1]^n\\ f_1(\mathbf{t})>0}} \left(\int_{\Gamma_2\in\mathbb{R}} \mathrm{e}(\Gamma_2 f_2(\mathbf{t}))\mathrm{d}\Gamma_2\right)\mathrm{d}\mathbf{t} = \mathfrak{J},&\end{aligned}$$

which concludes the proof. □

The integral part of Lemma 3.2.3 is calculated in successive steps by Lemmas 3.3.7, 3.4.4 and 3.4.5. Hence we may now turn our attention to the summation part. Recall the definition of $S_{\mathbf{a},q}$ and $\mathfrak{F}(a_1,q)$ respectively in (3.13) and (3.21) and let

$$\mathbb{L}_\phi := \sum_{q\in\mathbb{Z}_{>0}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q}\overline{\mathfrak{F}(a_1,q)}. \tag{3.34}$$

Under the assumptions of Theorem 3.1.3, the sum $\mathbb{L}_\phi$ converges absolutely since by (3.25) and (3.28) we have for all $x > 1$:

$$\begin{aligned}\sum_{\substack{q\in\mathbb{Z}_{>0}\\ q>x}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \left|S_{\mathbf{a},q}\overline{\mathfrak{F}(a_1,q)}\right| &\ll \sum_{\substack{q\in\mathbb{Z}_{>0}\\ q>x}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} q^{n-3-\lambda_0}\\ &\leq \sum_{\substack{q\in\mathbb{Z}_{>0}\\ q>x}} q^{-1-\lambda_0} \ll x^{-\lambda_0}.\end{aligned} \tag{3.35}$$

Lemma 3.4.6. *Under the assumptions of Theorem 3.1.3, any $P \geq 2$ validates*

$$\Theta_{\mathbb{Q}}(P) = \mathcal{C}_0\mathfrak{J}\frac{\mathbb{L}_\phi\sqrt{2}}{d^{1/2}}\frac{P^{n-d}}{(\log P)^{1/2}} + O\left((\log P)^{-\frac{1}{40}\frac{1}{(d-1)2^{d+2}}}\frac{P^{n-d}}{(\log P)^{1/2}}\right).$$

Proof. Combining Lemmas 3.3.7 and 3.4.2 shows

$$\frac{\Theta_{\mathbb{Q}}(P)}{P^{n-d}} = 2^{1/2}\mathcal{C}_0\mathcal{R}_1\mathcal{R}_2 + \mathcal{R}_3 + O\big((\log P)^{-1/2-\min\{A_1\lambda_0, A_2/2\}}\big), \tag{3.36}$$

with

$$\mathcal{R}_1 := \sum_{q\le(\log P)^{A_1}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q}\overline{\mathfrak{F}(a_1,q)},$$

$$\mathcal{R}_2 := \int_{|\mathbf{\Gamma}|\le(\log P)^{A_2}} \frac{I(\mathbf{\Gamma})}{P^d}\Big(\int_2^{\max\{f_1([-1,1]^n)\}P^d} \frac{\mathrm{e}(-\Gamma_1 P^{-d}t)}{\sqrt{\log t}}\mathrm{d}t\Big)\mathrm{d}\mathbf{\Gamma},$$

and where $\mathcal{R}_3$ is a quantity that satisfies

$$\mathcal{R}_3 \ll \sum_{q\le(\log P)^{A_1}} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{|S_{\mathbf{a},q}|}{q^n}\int_{|\mathbf{\Gamma}|\le(\log P)^{A_2}} \frac{|I(\mathbf{\Gamma})|}{P^d}\frac{q^3(1+|\Gamma_1|)P^d}{(\log P)^{1/2+1/7}}\mathrm{d}\mathbf{\Gamma}.$$

Bounding q and Γ_1 in the integrand by $(\log P)^{A_1}$ and $(\log P)^{A_2}$ respectively, we find

$$\mathcal{R}_3 \ll_{A_2} \frac{(\log P)^{3A_1+A_2}}{(\log P)^{1/2+1/7}} \sum_{q\le(\log P)^{A_1}} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{|S_{\mathbf{a},q}|}{q^n}\int_{|\mathbf{\Gamma}|\le(\log P)^{A_2}} |I(\mathbf{\Gamma})|\mathrm{d}\mathbf{\Gamma}.$$

By (3.27) and (3.28) the sum over q is convergent, and so is the integral over $\mathbf{\Gamma}$. Therefore we bound

$$\mathcal{R}_3 \ll_{A_2} (\log P)^{3A_1+A_2-1/2-1/7}. \tag{3.37}$$

Notice that $\mathcal{R}_2$ and $\mathcal{R}_1$ are truncated versions of $\mathfrak{J}_\phi(P)$ and $\mathbb{L}_\phi$ respectively. Next we will estimate the parts that are cut off. Using (3.27) we infer

$$\begin{aligned}
&\int_{|\mathbf{\Gamma}|>(\log P)^{A_2}} \frac{|I(\mathbf{\Gamma})|}{P^d}\Big(\int_2^{\max\{f_1([-1,1]^n)\}P^d} \frac{\mathrm{e}(-\Gamma_1 P^{-d}t)}{\sqrt{\log t}}\mathrm{d}t\Big)\mathrm{d}\mathbf{\Gamma}\\
\ll\ &\int_{|\mathbf{\Gamma}|>(\log P)^{A_2}} |I(\mathbf{\Gamma})|\frac{1}{\sqrt{\log P}}\mathrm{d}\mathbf{\Gamma}\\
\ll_{A_2}\ &(\log P)^{-1/2-A_2/2},
\end{aligned}$$

where in going from the first to the second line in the above, we have again bounded $|\,\mathrm{e}(\cdot)|$ by 1, and we bounded $P^{-d}\int_2^{\max\{f_1([-1,1]^n)\}P^d}(\log t)^{-1/2}\mathrm{d}t$ by application of Lemma 3.4.3.

Therefore we have

$$\mathcal{R}_2 = \mathfrak{J}_\phi(P) + O_{A_2}((\log P)^{-1/2-A_2/2}). \tag{3.38}$$

Furthermore, by (3.35) we deduce

$$\mathcal{R}_1 = \mathbb{L}_\phi + O_{A_1}((\log P)^{-A_1\lambda_0}). \tag{3.39}$$

We have already seen just before Lemma 3.4.4 that we have

$$\mathfrak{J}_\phi(P) \ll (\log P)^{-1/2},$$

thus injecting (3.37), (3.38) and (3.39) into (3.36) provides us with

$$\frac{\Theta_{\mathbb{Q}}(P)}{P^{n-d}} = 2^{1/2}\mathcal{C}_0\mathfrak{J}_\phi(P)\mathbb{L}_\phi + O((\log P)^{-1/2-\beta}),$$

with $\beta := \min\{A_1\lambda_0, A_2/2, -3A_1 - A_2 + 1/7\}$. A moment's thought affirms that assumption (3.1) ensures the validity of $\lambda_0 \geq (d-1)^{-1}2^{-d-2}$ and choosing $A_1 = \frac{1}{40} = A_2/2$ gives $\beta \geq (40(d-1)2^{d+2})^{-1}$. Finally, using Lemmas 3.4.4 and 3.4.5 concludes the proof. □

3.4.3 Proof of Theorem 3.1.3

Define

$$c_\phi := \frac{\mathfrak{J}}{d^{1/2}}\frac{2^{1/2}}{\zeta(n-d)}\frac{\mathbb{L}_\phi}{2}\mathcal{C}_0. \tag{3.40}$$

By Lemmas 3.2.1 and 3.4.6 the quantity $N(\phi, t)$ equals

$$\frac{\sqrt{2}}{2}\mathcal{C}_0\mathfrak{J}\mathbb{L}_\phi\frac{t^{n-d}}{d^{1/2}}\sum_{l\leq\log t}\frac{\mu(l)}{l^{n-d}(\log(t/l))^{1/2}}$$

up to an error term that is

$$\ll \frac{t^{n-d}}{\log t} + \sum_{l\leq\log t}\frac{(t/l)^{n-d}}{(\log(t/l))^{\frac{1}{2}+\frac{1}{40}\frac{1}{(d-1)2^{d+2}}}} \ll \frac{t^{n-d}}{(\log t)^{\frac{1}{2}+\frac{1}{40}\frac{1}{(d-1)2^{d+2}}}},$$

where the last estimate in the previous line is established as follows. First notice that the term $\frac{t^{n-d}}{\log t}$ falls under the estimate. For the sum we need to do a little bit more work. We begin with

$$\begin{aligned}\log(t/l) &= \log t - \log l\\ &\geq \log t\left(1 - \frac{\log\log t}{\log t}\right)\\ &\gg \log t,\end{aligned}$$

which allows us to take the denominator out of the sum. We moreover take t^{n-d} out of the sum, and then we notice that for $n-d \geq 2$ (which is valid because of (3.1)) the series $\sum_{l=1}^{\infty} l^{d-n}$ converges, so we may as well complete the sum and bound it by a constant.

Note that for $l \leq \log t$ we have $(\log(t/l))^{-1/2} = (\log t)^{-1/2} + O((\log t)^{-1})$, hence

$$\sum_{l \leq \log t} \frac{\mu(l)}{l^{n-d}(\log(t/l))^{1/2}} = (\log t)^{-1/2} \left(\sum_{l \leq \log t} \frac{\mu(l)}{l^{n-d}} \right) + O((\log t)^{-1}),$$

where the sum disappeared into the error term by completing to the range $l \in \mathbb{Z}_{>0}$, which gives a series converging to $\zeta(n-d)^{-1}$.

For the sum in the main term we use the completed sum again, but we include the error term arising from the cut-off, i.e.

$$\sum_{l \leq \log t} \frac{\mu(l)}{l^{n-d}} = \sum_{l=1}^{\infty} \frac{\mu(l)}{l^{n-d}} - \sum_{l > \log t} \frac{\mu(l)}{l^{n-d}} = \zeta(n-d)^{-1} + O\left(\frac{1}{(\log t)^{n-d-1}} \right)$$

where from the tail of the sum we arrive at the error term by bounding $|\mu(l)| \leq 1$ and comparing the sum to an integral, similarly to Lemma 3.4.3. Putting these arguments together we obtain

$$\sum_{l \leq \log t} \frac{\mu(l)}{l^{n-d}(\log(t/l))^{1/2}} = \zeta(n-d)^{-1}(\log t)^{-1/2} + O((\log t)^{-1})$$

and therefore

$$\frac{N(\phi, t)}{t^{n-d}(\log t)^{-1/2}} - \frac{\mathfrak{J}\mathbb{L}_{\phi}\mathcal{C}_0}{\zeta(n-d)\sqrt{2d}} \ll \frac{1}{(\log t)^{\varepsilon_d}}, \tag{3.41}$$

which concludes our proof. □

3.5 Interpretation of the leading constant

The circle method and the half-dimensional sieve allowed us to obtain a proof of the asymptotic in a technical, yet straightforward manner. However, this came at a cost because the leading constant c_{ϕ} in (3.40) is complicated. In this section we shall give an interpretation of c_{ϕ} via certain p-adic densities; this will not be straightforward.

In §3.5.1 we shall write $\mathbb{L}_\phi$ as an Euler product over all primes, with each factor involving complete exponential sums. Next, in §3.5.2 we shall show that for primes $p \equiv 3 \pmod 4$ these factors are connected to a particular kind of p-adic density. An analogous result will be proved in §3.5.3 for the prime 2. Finally, putting all partial results of §3.5 together, we shall provide in §3.5.4 an interpretation of the leading constant in Theorem 3.1.3, see Theorem 3.5.23.

3.5.1 Factorising $\mathbb{L}_\phi$

LEMMA 3.5.1. *For every integer $q \geq 3$ we have*

$$\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3 (\mathrm{mod}\ 4)}} \frac{\gcd(2^t k^2, q)}{2^t k^2} \ll q^{\frac{1}{\log\log q}}.$$

Proof. By multiplicativity the sum in the lemma equals

$$\left(\sum_{t=0}^{\infty} \frac{\gcd(2^t, q)}{2^t}\right) \prod_{p\equiv 3 (\mathrm{mod}\ 4)} \left(\sum_{i=0}^{\infty} \frac{\gcd(p^{2i}, q)}{p^{2i}}\right).$$

The sum over t is easily seen to be $2 + v_2(q)$, while the sum over i equals

$$\begin{cases} \frac{1+v_p(q)}{2} + \frac{p}{p^2-1}, & \text{if } 2 \nmid v_p(q), \\ 1 + \frac{v_p(q)}{2} + \frac{1}{p^2-1}, & \text{if } 2 \mid v_p(q). \end{cases}$$

This is at most $(1+v_p(q))(1+\frac{1}{p^2-1})$, hence we obtain the following bound for the sum in the lemma:

$$(2+v_2(q)) \prod_{p\neq 2} \Big[\big(1+(p^2-1)^{-1}\big)(1+v_p(q))\Big] \ll (2+v_2(q)) \frac{\tau(q)}{(1+v_2(q))} \leq 2\tau(q),$$

where τ is the divisor function. Using (3.4) allows to conclude the proof. □

For $q \in \mathbb{Z}_{>0}$, $a_1 \in \mathbb{Z} \cap [0, q)$ and $(k, t) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\geq 0}$, we define

$$T_{a_1,q}(t,k) := \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ \gcd(2^t k^2,q)|\ell\\ (3.22)}} \frac{\varpi(\gcd(\ell,q)/\gcd(2^t k^2,q))\, \mathrm{e}(-a_1\ell/q)}{\gcd(\ell,q)\mathrm{lcm}(4, q/\gcd(\ell,q))} \prod_{\substack{p\equiv 3 (\mathrm{mod}\ 4)\\ v_p(q)>v_p(\ell)}} \Big(1-\frac{1}{p}\Big)^{-1} \tag{3.42}$$

and we furthermore let

$$\mathbb{L}_{\phi}(k,t) := \sum_{q\in\mathbb{Z}_{>0}} \frac{\gcd(2^t k^2, q)}{q^n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} T_{a_1,q}(t,k). \tag{3.43}$$

LEMMA 3.5.2. *Under the assumptions of Theorem 3.1.3 we have*

$$\mathbb{L}_{\phi} = \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3(\mathrm{mod}\ 4)}} \frac{\mathbb{L}_{\phi}(k,t)}{k^2 2^t}.$$

Proof. The lemma follows immediately by combining (3.21) with (3.34) and inverting the order of summation, provided that one proves

$$\sum_{q\in\mathbb{Z}_{>0}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} |S_{\mathbf{a},q}| \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3(\mathrm{mod}\ 4)}} \frac{\gcd(2^t k^2, q)}{2^t k^2} |T_{a_1,q}(t,k)| < \infty.$$

To bound $T_{a_1,q}(t,k)$, observe that every prime p in the product in (3.42) must necessarily divide q, hence the product is at most

$$\prod_{p|q} \Big(1-\frac{1}{p}\Big)^{-1} = \frac{q}{\varphi(q)} \ll \log\log q,$$

where we used (3.5). Recalling $\varpi(m) \in \{0,1\}$ for all m and using the obvious bound $\mathrm{lcm}(4,b) \geq b$, valid for all $b \in \mathbb{Z}_{>0}$, we obtain the following bound with an absolute implied constant,

$$T_{a_1,q}(t,k) \ll \sum_{\ell\in\mathbb{Z}\cap[0,q)} \frac{1}{q} \log\log q = \log\log q.$$

Using this with Lemma 3.5.1 and (3.28) concludes the proof. □

In Lemmas 3.5.3–3.5.6, we show that for fixed a_1, t and k, the expression $T_{a_1,q}(t,k)$ can be analysed according to the prime factorisation of q. Before stating the lemmas we introduce the following notation. Recall the notation (3.19) and for $t, a \in \mathbb{Z}_{\geq 0}$, $q \in \mathbb{Z}_{>0}$ define

$$\mathcal{K}_{a,q}(t) := \sum_{\substack{\ell\in\mathbb{Z}\cap[0,2^{v_2(q)}),(3.44)\\ \gcd(\ell,2^{v_2(q)})=2^{\min\{t,v_2(q)\}}}} \mathrm{e}(-a\ell/2^{v_2(q)}),$$

with the summation condition

$$\frac{2^t}{2^{\min\{t,v_2(q)\}}} \equiv \frac{\ell\ddot{q}}{2^{\min\{t,v_2(q)\}}} \left(\mathrm{mod}\ 2^{\min\{2,v_2(q)-\min\{t,v_2(q)\}\}}\right). \tag{3.44}$$

For $a \in \mathbb{Z}_{\geq 0}$ and $q, k \in \mathbb{Z}_{>0}$ we furthermore let

$$\mathcal{W}_{a,q}(k) := \sum_{\substack{\ell \in \mathbb{Z} \cap [0,q) \\ \gcd(\ell,q)=\gcd(k^2,q)}} \mathrm{e}(-a\ell/q) \prod_{\substack{p \text{ prime} \\ v_p(q)>v_p(\ell)}} \left(1-\frac{1}{p}\right)^{-1}. \tag{3.45}$$

It is clear that if c is an integer coprime to q then we have

$$\mathcal{W}_{ca,q}(k) = \mathcal{W}_{a,q}(k). \tag{3.46}$$

LEMMA 3.5.3. *For all $k \in \mathbb{Z}_{>0}$ satisfying $k = \ddot{k}$, all $a, t \in \mathbb{Z}_{\geq 0}$ and $q \in \mathbb{Z}_{>0}$ we have*

$$T_{a,q}(t,k) = \frac{\mathcal{K}_{a,q}(t)}{2^{\min\{t,v_2(q)\}}\mathrm{lcm}(4, 2^{v_2(q)-\min\{t,v_2(q)\}})} \frac{\mathcal{W}_{a,\ddot{q}}(k)}{\ddot{q}} \times \begin{cases} 1, & \text{if } \dot{q} \mid a, \\ 0, & \text{if } \dot{q} \nmid a. \end{cases}$$

Proof. We observe that $T_{a_1,q}(t,k)$ equals

$$\sum_{\substack{\ell \in \mathbb{Z} \cap [0, 2^{v_2(q)}\dot{q}\ddot{q}) \\ \gcd(2^t k^2, 2^{v_2(q)}\ddot{q}) \mid \ell}} \frac{\varpi(\gcd(\ell, 2^{v_2(q)}\dot{q}\ddot{q})/\gcd(2^t k^2, 2^{v_2(q)}\ddot{q}))\, \mathrm{e}(-a_1\ell/(2^{v_2(q)}\dot{q}\ddot{q}))}{\gcd(\ell, 2^{v_2(q)}\dot{q}\ddot{q})\mathrm{lcm}(4, 2^{v_2(q)}\dot{q}\ddot{q}/\gcd(\ell, 2^{v_2(q)}\dot{q}\ddot{q}))}$$
$$\times \prod_{\substack{p \text{ prime} \\ v_p(\ddot{q})>v_p(\ell)}} \left(1-\frac{1}{p}\right)^{-1},$$

where the sum is over ℓ with

$$\frac{2^t k^2}{\gcd(2^t k^2, 2^{v_2(q)}\ddot{q})} \equiv \frac{\ell}{\gcd(\ell, 2^{v_2(q)}\dot{q}\ddot{q})} \left(\mathrm{mod}\ \gcd\left(4, \frac{2^{v_2(q)}}{\gcd(\ell, 2^{v_2(q)})}\right)\right).$$

We now use the fact that replacing ℓ by $\ell + 2^{v_2(q)}\dot{q}\ddot{q}$ leaves the last sum invariant. The Chinese remainder theorem allows to uniquely write

$$\ell \equiv \ell_1\dot{q}\ddot{q} + \ell_2 2^{v_2(q)}\ddot{q} + \ell_3 2^{v_2(q)}\dot{q} \left(\mathrm{mod}\ 2^{v_2(q)}\dot{q}\ddot{q}\right)$$

for some

$$\ell_1 \in \mathbb{Z} \cap [0, 2^{v_2(q)}),\ \ell_2 \in \mathbb{Z} \cap [0, \dot{q}) \text{ and } \ell_3 \in \mathbb{Z} \cap [0, \ddot{q}).$$

Then $T_{a_1,q}(t,k)$ becomes

$$\sum_{\substack{\ell_1\in\mathbb{Z}\cap[0,2^{v_2(q)})\\ \ell_2\in\mathbb{Z}\cap[0,\dot q)\\ \ell_3\in\mathbb{Z}\cap[0,\dot q)\\ \gcd(k^2,\ddot q)\mid\ell_3\\ 2^{\min\{t,v_2(q)\}}\mid\ell_1}} \frac{\varpi\big(\frac{\gcd(\ell_1,2^{v_2(q)})}{2^{\min\{t,v_2(q)\}}}\gcd(\ell_2,\dot q)\frac{\gcd(\ell_3,\ddot q)}{\gcd(k^2,\ddot q)}\big)\,\mathrm{e}\big(\frac{-a_1\ell_1}{2^{v_2(q)}}\big)\,\mathrm{e}\big(\frac{-a_1\ell_2}{\dot q}\big)\,\mathrm{e}\big(\frac{-a_1\ell_3}{\ddot q}\big)}{\gcd(\ell_1,2^{v_2(q)})\mathrm{lcm}(4,2^{v_2(q)}/\gcd(\ell_1,2^{v_2(q)}))\dot q\ddot q}$$

$$\times \prod_{\substack{p\text{ prime}\\ v_p(\ddot q)>v_p(\ell_3)}}\Big(1-\frac{1}{p}\Big)^{-1},$$

where the sum is over ℓ_1,ℓ_3 with

$$\frac{2^{t-\min\{t,v_2(q)\}}}{\gcd(k^2,\ddot q)}\equiv\frac{\ell_1\ddot q}{\gcd(\ell_1,2^{v_2(q)})\gcd(\ell_3,\ddot q)}\left(\mathrm{mod}\ \gcd\Big(4,\frac{2^{v_2(q)}}{\gcd(\ell_1,2^{v_2(q)})}\Big)\right).$$

Indeed, modulo $\gcd\Big(4,\frac{2^{v_2(q)}}{\gcd(\ell_1,2^{v_2(q)})}\Big)$, the term $\ell_2 2^{v_2(q)}\ddot q+\ell_3 2^{v_2(q)}\dot q$ vanishes. Note furthermore that we have used that each of k^2, $\dot q$ and $\gcd(\ell_2,\dot q)$ is $1\,(\mathrm{mod}\ 4)$. This holds because k is odd and each prime divisor of $\dot q$ is $1\,(\mathrm{mod}\ 4)$. Moreover, the presence of the $\varpi(\cdot)$ means that we may freely restrict to the case

$$\gcd(\ell_1,2^{v_2(q)})=2^{\min\{t,v_2(q)\}}\ \text{and}\ \gcd(\ell_3,\ddot q)=\gcd(k^2,\ddot q).$$

Put together, these two facts show that $T_{a_1,q}(t,k)$ equals

$$\frac{\mathcal{K}_{a_1,q}(t)}{2^{\min\{t,v_2(q)\}}\mathrm{lcm}(4,2^{v_2(q)-\min\{t,v_2(q)\}})}\frac{\mathcal{W}_{a_1,\ddot q}(k)}{\ddot q}\frac{1}{\dot q}\sum_{\ell_2\in\mathbb{Z}/\dot q\mathbb{Z}}\mathrm{e}(-a_1\ell_2/\dot q),$$

thus concluding the proof. □

Essentially, the last lemma breaks up the information of the prime 2, carried by the factor involving $\mathcal{K}_{a,q}(t)$, and the information on the primes $p\equiv 3\,(\mathrm{mod}\ 4)$, carried by the factor involving $\mathcal{W}_{a,\ddot q}(k)$. The last factor with values in $\{0,1\}$ sieves out possible values of a for any given q and arises from a Ramanujan sum in the last line of the proof.

LEMMA 3.5.4. *For fixed $k\in\mathbb{Z}_{>0}$, $a\in\mathbb{Z}$ the function $\mathcal{W}_{a,q}(k)$ is multiplicative with respect to q.*

Proof. For positive coprime integers q_1 and q_2 we note that any element $\ell \in \mathbb{Z}/q_1q_2\mathbb{Z}$ can be written uniquely as $\ell_1 q_2 + \ell_2 q_1$, for $\ell_1 \in \mathbb{Z}/q_1\mathbb{Z}$ and $\ell_2 \in \mathbb{Z}/q_2\mathbb{Z}$. From this the validity of $\mathcal{W}_{a,q_1q_2}(k) = \mathcal{W}_{a,q_1}(k)\mathcal{W}_{a,q_2}(k)$ follows easily. □

Before we state the next lemma, recall the Ramanujan sum from (3.6).

LEMMA 3.5.5. *For fixed $a, m \in \mathbb{Z}_{\geq 0}$, $k \in \mathbb{Z}_{>0}$, and any prime p define $j := m - 2v_p(k)$. Then we have*

$$\mathcal{W}_{a,p^m}(k) = \begin{cases} c_{p^j}(-a)(1-1/p)^{-1}, & \text{if } 2v_p(k) < m, \\ 1, & \text{if } 2v_p(k) \geq m. \end{cases}$$

Proof. For $2v_p(k) \geq m$, only the term $\ell = 0$ contributes towards $\mathcal{W}_{a,p^m}(k)$, in which case the sum equals 1. For $0 \leq 2v_p(k) < m$, every ℓ in (3.45) must be of the form $\ell = xp^{2v_p(k)}$, where $x \in \mathbb{Z} \cap [0, p^j)$ and $p \nmid x$ hold, which concludes the proof. □

Define for $a, \varrho, t \in \mathbb{Z}_{\geq 0}$ the symbol

$$\Lambda_{a,\varrho}(t) := \mathrm{e}(-a/2^{\varrho-t})\mathbf{1}_{v_2(a)\geq \varrho-t-2}. \tag{3.47}$$

LEMMA 3.5.6. *For $q \in \mathbb{Z}_{>0}$, let q_0 be any integer satisfying the congruence $q_0 \equiv \ddot{q} \pmod{2^{\min\{2,v_2(q)\}}}$. Then for all $a, t \in \mathbb{Z}_{\geq 0}$ and $q \in \mathbb{Z}_{>0}$ we have*

$$\frac{\mathcal{K}_{a,q}(t)}{\mathrm{lcm}(4, 2^{v_2(q)-\min\{t,v_2(q)\}})} = \frac{\Lambda_{aq_0,v_2(q)}(t)}{4}.$$

Proof. If $v_2(q) \leq t$ holds then we have

$$\mathcal{K}_{a,q}(t) = \sum_{\substack{\ell \in \mathbb{Z}\cap[0,2^{v_2(q)}) \\ 2^{v_2(q)}\mid \ell}} \mathrm{e}(-a\ell/2^{v_2(q)}) = 1,$$

so the left-hand side equals 1/4. On the right-hand side of the equation, we see that $v_2(q)-t-2$ is negative, so $v_2(aq_0)$ is certainly larger. Moreover, $-aq_0/2^{t-v_2(q)}$ is an integer. Hence both the exponential and the indicator take the value 1.

If $v_2(q) > t$ holds then we have

$$\begin{aligned}\mathcal{K}_{a,q}(t) &= \sum_{\substack{\ell \in \mathbb{Z} \cap [0, 2^{v_2(q)}) \\ 2^t \mid \ell, 2^{t+1} \nmid \ell \\ 1 \equiv \frac{\ell \ddot{q}}{2^t} \left(\mathrm{mod}\ 2^{\min\{2, v_2(q)-t\}}\right)}} \mathrm{e}(-a\ell/2^{v_2(q)}) \\ &= \sum_{\substack{x \in \mathbb{Z} \cap [0, 2^{v_2(q)-t}) \\ x \equiv \ddot{q} \left(\mathrm{mod}\ 2^{\min\{2, v_2(q)-t\}}\right)}} \mathrm{e}(-ax/2^{v_2(q)-t}),\end{aligned}$$

where the condition $x \equiv \ddot{q}$ is equivalent to $1 \equiv x\ddot{q}$ as $\ddot{q}^2 \equiv 1 \,(\mathrm{mod}\ 2)$ and $\ddot{q}^2 \equiv 1 \,(\mathrm{mod}\ 4)$ hold.

If $v_2(q) - t$ equals 1 then this becomes $\mathrm{e}(a/2)$, while, for $v_2(q) - t = 2$ this is equal to $\mathrm{e}(-a\ddot{q}/4)$. In the remaining cases we have $v_2(q) - t > 2$, hence also

$$\begin{aligned}\mathcal{K}_{a,q}(t) &= \sum_{\substack{x \in \mathbb{Z} \cap [0, 2^{v_2(q)-t}) \\ x \equiv \ddot{q} (\mathrm{mod}\ 4)}} \mathrm{e}(-ax/2^{v_2(q)-t}) \\ &= \mathrm{e}(-a\ddot{q}/2^{v_2(q)-t}) \sum_{y \in \mathbb{Z} \cap [0, 2^{v_2(q)-t-2})} \mathrm{e}(-ay/2^{v_2(q)-t-2}),\end{aligned}$$

which vanishes in case a is not a multiple of $2^{v_2(q)-t-2}$ and otherwise equals $\mathrm{e}(-a\ddot{q}/2^{v_2(q)-t})2^{v_2(q)-t-2}$. □

For each a and q having separated out the contributions to $T_{a,q}(t,k)$, we now do the same for their sums (weighted by $S_{\mathbf{a},q}$) over all possible values of $\mathbf{a}$ for given q.

LEMMA 3.5.7. *For all $k, q \in \mathbb{Z}_{>0}$ with $k = \ddot{k}$ and all $t \in \mathbb{Z}_{\geq 0}$ we have*

$$\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q}T_{a_1,q}(t,k) = \frac{1}{2^{2+\min\{t,v_2(q)\}}} \times \left(\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{v_2(q)}))^2\\ \gcd(b_1,b_2,2^{v_2(q)})=1}} S_{\mathbf{b},2^{v_2(q)}}\Lambda_{b_1,v_2(q)}(t) \right) \times \left(\sum_{\substack{b\in\mathbb{Z}\cap[0,\dot{q})\\ \gcd(b,\dot{q})=1}} \sum_{\mathbf{t}\in(\mathbb{Z}/\dot{q}\mathbb{Z})^n} \mathrm{e}\left(bf_2(\mathbf{t})/\dot{q}\right) \right) \times \left(\frac{1}{\ddot{q}} \sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,\ddot{q}))^2\\ \gcd(b_1,b_2,\ddot{q})=1}} S_{\mathbf{b},\ddot{q}}\mathcal{W}_{b_1,\ddot{q}}(k) \right).$$

Proof. By the Chinese remainder theorem we can uniquely write every $a_i \in \mathbb{Z}/q\mathbb{Z}$ as

$$a_i \equiv a_i'\dot{q}\ddot{q} + a_i''2^{v_2(q)}\ddot{q} + a_i'''2^{v_2(q)}\dot{q} \pmod{q}, \ (i = 1, 2),$$

with

$$a_i' \in \mathbb{Z}/2^{v_2(q)}\mathbb{Z}, a_i'' \in \mathbb{Z}/\dot{q}\mathbb{Z}, a_i''' \in \mathbb{Z}/\ddot{q}\mathbb{Z}.$$

Thus we see that the sum over $\mathbf{a} \in (\mathbb{Z} \cap [0, q))^2$ in the lemma equals

$$\sum_{\substack{\mathbf{a}''\in(\mathbb{Z}\cap[0,\dot{q}))^2,\gcd(a_1'',a_2'',\dot{q})=1\\ \mathbf{a}'''\in(\mathbb{Z}\cap[0,\ddot{q}))^2,\gcd(a_1''',a_2''',\ddot{q})=1\\ \mathbf{a}'\in(\mathbb{Z}\cap[0,2^{v_2(q)}))^2,\gcd(a_1',a_2',2^{v_2(q)})=1}} S_{\mathbf{a}'\dot{q}\ddot{q}+\mathbf{a}''2^{v_2(q)}\ddot{q}+\mathbf{a}'''2^{v_2(q)}\dot{q},2^{v_2(q)}\dot{q}\ddot{q}} \times T_{a_1'\dot{q}\ddot{q}+a_1''2^{v_2(q)}\ddot{q}+a_1'''2^{v_2(q)}\dot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t,k).$$

It is easy to check that whenever q_1 and q_2 are coprime positive integers and $\mathbf{a} \in \mathbb{Z}^2$, then, much like as in the proof of Lemma 1.3.11, we have

$$S_{\mathbf{a},q_1q_2} = S_{q_2^{d-1}\mathbf{a},q_1}S_{q_1^{d-1}\mathbf{a},q_2},$$

by the fact that for fixed $r \in \mathbb{Z}_{>0}$ the sum $S_{\mathbf{b},r}$ only depends on $\mathbf{b} \pmod{r}$.

From the above, we see that if q_1, q_2, q_3 are any positive integers that are coprime in pairs then we have

$$S_{\mathbf{a},q_1q_2q_3} = S_{(q_2q_3)^{d-1}\mathbf{a},q_1} S_{(q_1q_3)^{d-1}\mathbf{a},q_2} S_{(q_1q_2)^{d-1}\mathbf{a},q_3}.$$

Applying this for $\mathbf{a} = \mathbf{a}'\dot{q}\ddot{q} + \mathbf{a}''2^{v_2(q)}\ddot{q} + \mathbf{a}'''2^{v_2(q)}\dot{q}$, $q_1 = 2^{v_2(q)}$, $q_2 = \dot{q}$ and $q_3 = \ddot{q}$, we obtain

$$S_{\mathbf{a}'\dot{q}\ddot{q}+\mathbf{a}''2^{v_2(q)}\ddot{q}+\mathbf{a}'''2^{v_2(q)}\dot{q},2^{v_2(q)}\dot{q}\ddot{q}} = S_{(\dot{q}\ddot{q})^d\mathbf{a}',2^{v_2(q)}} S_{(2^{v_2(q)}\ddot{q})^d\mathbf{a}'',\dot{q}} S_{(2^{v_2(q)}\dot{q})^d\mathbf{a}''',\ddot{q}},$$

where we again made use of the fact that for fixed $r \in \mathbb{Z}_{>0}$ the sum $S_{\mathbf{b},r}$ only depends on $\mathbf{b} \pmod r$, as we will also do for $\mathcal{W}_{a,q}(k)$ and $\mathcal{K}_{a,q}(t)$ below.

By Lemma 3.5.3 one sees that $T_{a_1'\dot{q}\ddot{q}+a_1''2^{v_2(q)}\ddot{q}+a_1'''2^{v_2(q)}\dot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t,k)$ equals

$$\frac{\mathcal{K}_{a_1'\dot{q}\ddot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t)}{2^{\min\{t,v_2(q)\}}\mathrm{lcm}\big(4, 2^{v_2(q)-\min\{t,v_2(q)\}}\big)} \frac{\mathcal{W}_{a_1'''2^{v_2(q)}\dot{q},\ddot{q}}(k)}{\ddot{q}} \times \begin{cases} 1, & \text{if } \dot{q} \mid a_1'', \\ 0, & \text{if } \dot{q} \nmid a_1'', \end{cases}$$

thus showing that the sum over $\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2$ in the lemma equals $\mathcal{L}'\mathcal{L}''\mathcal{L}'''$, where we write

$$\mathcal{L}' := \sum_{\substack{\mathbf{a}' \in (\mathbb{Z}\cap[0,2^{v_2(q)}))^2 \\ \gcd(a_1',a_2',2^{v_2(q)})=1}} S_{(\dot{q}\ddot{q})^d\mathbf{a}',2^{v_2(q)}} \frac{\mathcal{K}_{a_1'\dot{q}\ddot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t)}{2^{\min\{t,v_2(q)\}}\mathrm{lcm}\big(4, 2^{v_2(q)-\min\{t,v_2(q)\}}\big)},$$

$$\mathcal{L}'' := \sum_{\substack{\mathbf{a}'' \in (\mathbb{Z}\cap[0,\dot{q}))^2, \dot{q} \mid a_1'' \\ \gcd(a_1'',a_2'',\dot{q})=1}} S_{(2^{v_2(q)}\ddot{q})^d\mathbf{a}'',\dot{q}},$$

$$\mathcal{L}''' := \sum_{\substack{\mathbf{a}''' \in (\mathbb{Z}\cap[0,\ddot{q}))^2 \\ \gcd(a_1''',a_2''',\ddot{q})=1}} S_{(2^{v_2(q)}\dot{q})^d\mathbf{a}''',\ddot{q}} \frac{\mathcal{W}_{a_1'''2^{v_2(q)}\dot{q},\ddot{q}}(k)}{\ddot{q}}.$$

To simplify $\mathcal{L}''$ we make an invertible change of variables, namely we will write $b \equiv (2^{v_2(q)}\ddot{q})^d a_2'' \pmod{\dot{q}}$. This results in

$$\mathcal{L}'' = \sum_{\substack{b \in \mathbb{Z}\cap[0,\dot{q}) \\ \gcd(b,\dot{q})=1}} \sum_{\mathbf{t} \in (\mathbb{Z}/\dot{q}\mathbb{Z})^n} \mathrm{e}\big(bf_2(\mathbf{t})/\dot{q}\big).$$

Similarly, for $\mathcal{L}'''$ we make the change of variables $\mathbf{b} \equiv (2^{v_2(q)}\dot{q})^d \mathbf{a}''' \pmod{\ddot{q}}$ and use (3.46) to show the validity of

$$cL''' = \frac{1}{\ddot{q}} \sum_{\substack{\mathbf{b} \in (\mathbb{Z} \cap [0,\ddot{q}))^2 \\ \gcd(b_1,b_2,\ddot{q})=1}} S_{\mathbf{b},\ddot{q}} \mathcal{W}_{b_1,\ddot{q}}(k).$$

Finally, put $\mathbf{b} \equiv (\dot{q}\ddot{q})^d \mathbf{a}' \pmod{2^{v_2(q)}}$ and find some $y \in \mathbb{Z}$ which satisfies $y\dot{q}\ddot{q} \equiv 1 \pmod{2^{v_2(q)}}$. Observing that $\dot{q}\ddot{q}a_1' \equiv b_1 y^{d-1} \pmod{2^{v_2(q)}}$ holds, we see $\mathcal{K}_{a_1'\dot{q}\ddot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t) = \mathcal{K}_{b_1 y^{d-1},2^{v_2(q)}\dot{q}\ddot{q}}(t)$. Note that d is even and that y is odd, hence the proof is concluded by application of Lemma 3.5.6 with $a = b_1 y^{d-1}$ and $q_0 := y^{d-1}$, made possible by the validity of

$$y^{d-1} \equiv y \equiv (\dot{q}\ddot{q})^{-1} \equiv \ddot{q} \pmod{2^{\min\{2,v_2(q)\}}}.$$

Indeed, we have $\Lambda_{b_1(y^{d-1})^2,v_2(q)}(t) = \Lambda_{b_1,v_2(q)}(t)$ since $\Lambda_{a,\varrho}(t)$ only depends on a through $a \pmod{2^{\varrho-t}}$. □

We will continue our journey in splitting into factors coming from different primes with $\mathbb{L}_\phi(k,t)$. We will first need some notation.

For $t \in \mathbb{Z}_{\geq 0}$ and $k \in \mathbb{Z}_{>0}$ with $\ddot{k} = k$ define

$$\Upsilon_1(k) := \sum_{\substack{q_3 \in \mathbb{Z}_{>0} \\ p|q_3 \Rightarrow p \equiv 3 \pmod 4}} \frac{\gcd(k^2,q_3)}{q_3^{n+1}} \sum_{\substack{\mathbf{b} \in (\mathbb{Z} \cap [0,q_3))^2 \\ \gcd(b_1,b_2,q_3)=1}} S_{\mathbf{b},q_3} \mathcal{W}_{b_1,q_3}(k) \tag{3.48}$$

and

$$\Upsilon_2(t) := \frac{1}{4} \sum_{\varrho \in \mathbb{Z}_{\geq 0}} \frac{1}{2^{\varrho n}} \sum_{\substack{\mathbf{b} \in (\mathbb{Z} \cap [0,2^\varrho))^2 \\ \gcd(b_1,b_2,2^\varrho)=1}} S_{\mathbf{b},2^\varrho} \Lambda_{b_1,\varrho}(t). \tag{3.49}$$

For a prime p define

$$\tau_{f_2}(p) := \lim_{N \to \infty} \frac{\#\{\mathbf{t} \in (\mathbb{Z} \cap [0,p^N))^n : f_2(\mathbf{t}) \equiv 0 \pmod{p^N}\}}{p^{N(n-1)}} \tag{3.50}$$

and let us now see why the limit exists. Our set-up and assumption (3.1) ensure that the work of Birch [Bir62] applies to the hypersurface $f_2 = 0$. In particular, the constant $K = K(f_2)$, defined in (1.6) equals $2^{1-d}n$ because f_2 has no singularities. Furthermore, one should notice that we have

$$\tau_{f_2}(p) = 1 + \sum_{m=1}^{\infty} \frac{1}{p^{mn}} \sum_{a \in (\mathbb{Z}/p^m\mathbb{Z})^*} \sum_{\mathbf{t} \in (\mathbb{Z} \cap [0,p^m))^n} \mathrm{e}\left(\frac{af_2(\mathbf{t})}{p^m}\right) \tag{3.51}$$

coming from the fact that

$$p^{N(n-1)}\sum_{m=0}^{N}\frac{1}{p^{mn}}\sum_{a\in(\mathbb{Z}/p^m\mathbb{Z})^*}\sum_{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n}\mathrm{e}\Big(\frac{af_2(\mathbf{t})}{p^m}\Big) \tag{3.52}$$

equals $\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^N))^n : f_2(\mathbf{t})\equiv 0\big(\mathrm{mod}\ p^N\big)\big\}$ and that the $m=0$ term equals 1. Alternatively, the existence of the limit $\tau_{f_2}(p)$ could be established by using Hensel's lemma and the fact that f_2 defines a smooth hypersurface over $\mathbb{Q}_p$.

Using Lemma 1.3.34 to bound the sum over $\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n$ by an order of magnitude $\ll_\varepsilon p^{m(\varepsilon-n+n(d-1)^{-1}2^{-d+1})}$ (valid for all fixed $\varepsilon>0$), shows that, when (3.1) is used in the form $n\geq 1+3(d-1)2^d$ and $\varepsilon=(d-1)^{-1}2^{-d+1}$ is taken, the last series over m converges absolutely. Therefore the limit in (3.50) exists. In addition we get

$$\tau_{f_2}(p)=1+O(p^{\varepsilon-5+(d-1)^{-1}2^{-d+1}})=1+O(p^{-2}). \tag{3.53}$$

Lemma 3.5.8. *Under the assumptions of Theorem 3.1.3, for all $t\in\mathbb{Z}_{\geq 0}$ and $k\in\mathbb{Z}_{>0}$ with $\ddot{k}=k$, the sums in* (3.48) *and* (3.49) *both converge absolutely. We furthermore have*

$$\mathbb{L}_\phi(k,t)=\Upsilon_1(k)\Upsilon_2(t)\prod_{p\equiv 1(\mathrm{mod}\ 4)}\tau_{f_2}(p).$$

Proof. The assumptions of Theorem 3.1.3 allow us to use the bound from equation (3.28), which, when combined with the bounds $\gcd(k^2,q_3)\leq k^2$ and $|\mathcal{W}_{b_1,q_3}(k)|\leq q_3$, shows that the sum over q_3 in (3.48) converges absolutely. To prove the analogous statement for the sum over ϱ in (3.49) we use the bound (3.28) as well as the inequality $|\Lambda_{b_1,\varrho}(t)|\leq 1$ that is apparent from (3.47).

To complete the proof of the lemma, we write each q in (3.43) as $q=2^\varrho q_1q_3$, denoting $q_1=\dot{q}$ and $q_3=\ddot{q}$ and we inject Lemma 3.5.7 into (3.43) to obtain $\mathbb{L}_\phi(k,t)=\Upsilon_1(k)\Upsilon_2(t)\Xi$, with

$$\Xi:=\sum_{\substack{q_1\in\mathbb{Z}_{>0}\\ p|q_1\Rightarrow p\equiv 1(\mathrm{mod}\ 4)}}\frac{1}{q_1^n}\sum_{b\in(\mathbb{Z}/q_1\mathbb{Z})^*}\sum_{\mathbf{t}\in(\mathbb{Z}/q_1\mathbb{Z})^n}\mathrm{e}\big(bf_2(\mathbf{t})/q_1\big).$$

It is standard that the sum over $b\in(\mathbb{Z}/q_1\mathbb{Z})^*$ forms a multiplicative function of q_1, see, for example, [Bir62, §7] with $R=1$ or Lemma 1.3.11. Thus, using the expression for $\tau_{f_2}(p)$ in (3.51), we obtain the equality of Ξ with the product over the primes $p\equiv 1\,(\mathrm{mod}\ 4)$ in the lemma. □

Let us now define the quantities $E_\phi(p)$ for every prime $p \equiv 3 \pmod 4$ and for $p = 2$ as follows: if $p \equiv 3 \pmod 4$ then we let

$$E_\phi(p) := \sum_{\kappa,m \in \mathbb{Z}_{\geq 0}} \Phi_{\kappa,m} p^{-2\kappa}, \tag{3.54}$$

with

$$\Phi_{\kappa,m} := \frac{\gcd(p^{2\kappa}, p^m)}{p^{m(n+1)}} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,p^m))^2 \\ \gcd(a_1,a_2,p^m)=1}} S_{\mathbf{a},p^m} \mathcal{W}_{a_1,p^m}(p^\kappa). \tag{3.55}$$

We furthermore define

$$E_\phi(2) := \frac{1}{4} \sum_{t,\varrho \in \mathbb{Z}_{\geq 0}} \frac{1}{2^t} \frac{1}{2^{\varrho n}} \sum_{\substack{\mathbf{b} \in (\mathbb{Z} \cap [0,2^\varrho))^2 \\ \gcd(b_1,b_2,2^\varrho)=1}} S_{\mathbf{b},2^\varrho} \, \mathrm{e}(-b_1 2^{t-\varrho}) \mathbf{1}_{v_2(b_1) \geq \varrho - t - 2}. \tag{3.56}$$

With this newest notation, we are finally ready to write $\mathbb{L}_\phi$ itself as a product of factors coming from each of the primes.

LEMMA 3.5.9. *Keep the assumptions of Theorem 3.1.3. Then the sums in* (3.54) *and* (3.56) *converge absolutely. In addition, the infinite product*

$$E_\phi(2) \Big(\prod_{p \equiv 1 \pmod 4} \tau_{f_2}(p) \Big) \Big(\prod_{p \equiv 3 \pmod 4} E_\phi(p) \Big)$$

converges absolutely and equals $\mathbb{L}_\phi$.

Proof. Our first task is to show that the sum in (3.54) converges absolutely. For this we use Lemma 3.5.5 and the obvious bound $|c_{p^j}(-a)| \leq p^j$ to obtain

$$|\mathcal{W}_{a_1,p^m}(p^\kappa)| \leq 2 \frac{p^m}{\gcd(p^{2\kappa}, p^m)}.$$

Therefore, by (3.28), for every $0 < \lambda < 2^{-d}(d-1)^{-1}$ we have

$$\Phi_{\kappa,m} \ll \frac{\gcd(p^{2\kappa}, p^m)}{p^{m(n+1)}} p^{2m} p^{m(n-3-\lambda)} \frac{p^m}{\gcd(p^{2\kappa}, p^m)} \ll_\lambda p^{-m(1+\lambda)},$$

with an implied constant that depends at most on λ, f_1 and f_2. This shows that for all integers $M \geq 0$ and every $0 < \lambda < 2^{-d}(d-1)^{-1}$ one has

$$\sum_{\kappa \geq 0} \frac{1}{p^{2\kappa}} \sum_{m \geq M} |\Phi_{\kappa,m}| \ll_\lambda \frac{1}{p^{M(1+\lambda)}}. \tag{3.57}$$

This completes our first task. The proof of the absolute convergence for the sum in (3.56) can be completed in a similar way by using (3.28) again. To show that the product over the primes $p \equiv 1 \,(\mathrm{mod}\, 4)$ in our lemma converges absolutely one can simply utilise (3.53). The product over the primes $p \equiv 3 \,(\mathrm{mod}\, 4)$ converges absolutely because the use of (3.57) with $M = 1$ and (3.54) yields

$$E_{\phi}(p) = \sum_{\kappa \in \mathbb{Z}_{\geq 0}} \Phi_{\kappa,0} p^{-2\kappa} + O(p^{-1-\lambda}) = \sum_{\kappa \in \mathbb{Z}_{\geq 0}} p^{-2\kappa} + O(p^{-1-\lambda})$$

and using $\sum_{\kappa \geq 0} p^{-2\kappa} = 1 + O(p^{-2})$ and $\lambda < 1$ provides us with

$$\lambda \in (0, 2^{-d}(d-1)^{-1}) \Rightarrow E_{\phi}(p) = 1 + O_{\lambda}(p^{-1-\lambda}). \tag{3.58}$$

Since for every $\lambda > 0$, the sum $\sum_{p \equiv 3 (\mathrm{mod}\ 4)} p^{-1-\lambda}$ converges absolutely, we conclude that so does the product $\prod_{p \equiv 3 (\mathrm{mod}\ 4)} E_{\phi}(p)$.

To prove the claimed equality of our lemma we combine Lemma 3.5.2 and Lemma 3.5.8 to obtain

$$\mathbb{L}_{\phi} = \Big(\sum_{t \in \mathbb{Z}_{\geq 0}} \frac{\Upsilon_2(t)}{2^t} \Big) \Big(\prod_{p \equiv 1 (\mathrm{mod}\ 4)} \tau_{f_2}(p) \Big) \Big(\sum_{\substack{k \in \mathbb{Z}_{>0} \\ p|k \Rightarrow p \equiv 3 (\mathrm{mod}\ 4)}} \frac{\Upsilon_1(k)}{k^2} \Big). \tag{3.59}$$

By (3.48) we can write the sum over $k \in \mathbb{Z}_{>0}$ as a double sum over k and q_3 and one obtains the infinite product over the primes $p \equiv 3 \,(\mathrm{mod}\, 4)$ in our lemma by application of a two-dimensional analogue for converting infinite sums into Euler products. Such an analogue can for example be found in [Hoo93, Lemma 4, pg.20] Lastly, the sum over t in (3.59) can be shown to be equal to $E_{\phi}(2)$ by application of (3.49). □

We are still left with interpreting the factors occurring in the last lemma. Before embarking on the next subsections we introduce some more notation and record some preparatory observations.

For primes p and integers $0 \leq i, j \leq m$ we define the quantity

$$\xi_{i,j}(m) := \#\big\{ \mathbf{t} \in (\mathbb{Z} \cap [0, p^m)^n : p^i \mid f_1(\mathbf{t}), p^j \mid f_2(\mathbf{t}) \big\}. \tag{3.60}$$

The quantity $\xi_{i,j}(m)$ also depends on p, however, we choose to not record this in the notation as it will be clear from the context what the underlying prime is. The following is a restatement of the last equation in [Bir62,

pg.259], and which we have already used in studying (3.50) for the case of a single polynomial, where we now have a pair:

$$\sum_{0\leq m\leq N}\frac{1}{p^{mn}}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ \gcd(a_1,a_2,p^m)=1}} S_{\mathbf{a},p^m}=\frac{\xi_{N,N}(N)}{p^{N(n-2)}}. \tag{3.61}$$

Using it for $m=N$ and $m=N-1$ both, we obtain that for every $N\in\mathbb{Z}_{>0}$ we have

$$\sum_{\substack{\mathbf{a}\in([0,p^N))^2\\ \gcd(a_1,a_2,p^N)=1}} S_{\mathbf{a},p^N}=p^{2N}\xi_{N,N}(N)-p^{2N+n-2}\xi_{N-1,N-1}(N-1). \tag{3.62}$$

Observe that injecting the bound (3.28) into (3.61) shows that for $M\geq 0$ we have

$$\xi_{M,M}(M)=O_p\big(p^{M(n-2)}\big). \tag{3.63}$$

Lemma 3.5.10. *Keep the assumptions of Theorem 3.1.3. Then for every $m_1,m_2,M\in\mathbb{Z}_{>0}$ with $m_1\leq m_2\leq M$, and every prime p we have*

$$\xi_{m_1,m_2}(M)=O_p(p^{Mn-2m_1}).$$

Proof. Notice that we have

$$\xi_{m_1,m_2}(M)\leq \#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^{m_1}))^n : p^{m_1}\mid f_1(\mathbf{t}), p^{m_1}\mid f_2(\mathbf{t})\big\}p^{n(M-m_1)}.$$

Thus using (3.63) we conclude that $\xi_{m_1,m_2}(M)=O_p(p^{m_1(n-2)}p^{n(M-m_1)})$. □

3.5.2 Local density at primes $3\,(\mathrm{mod}\,4)$

The following is the main result of this section.

Proposition 3.5.11. *Let p be a prime number with $p\equiv 3\,(\mathrm{mod}\,4)$. Then under the assumptions of Theorem 3.1.3, the sequence*

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^N))^n : f_2(\mathbf{t})\equiv 0\,(\mathrm{mod}\,p^N), x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \text{ has a } \mathbb{Q}_p\text{-point}\big\}}{p^{N(n-1)}}$$

has a limit for $N\to\infty$. We call the value of this limit ℓ_p and we have $E_\phi(p)=\big(1-1/p\big)^{-1}\ell_p$.

For the rest of §3.5.2 the letter p will always refer to a prime satisfying $p \equiv 3 \pmod 4$. To prove Proposition 3.5.11 we split the sum over κ and m in the definition of $E_\phi(p)$ according to the three ranges $0 \le m \le 2\kappa$, $m = 2\kappa + 1$ and $m \ge 2\kappa + 2$. These ranges will be treated in Lemmas 3.5.12, 3.5.13 and 3.5.16 respectively.

LEMMA 3.5.12. *Keep the assumptions of Theorem 3.1.3. Then for every prime $p \equiv 3 \pmod 4$ and $M \in \mathbb{Z}_{>0}$ the following holds,*

$$\sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \sum_{0 \le m \le \min\{M, 2\kappa\}} \Phi_{\kappa,m} = \sum_{\kappa \ge 0} \frac{\xi_{2\kappa,2\kappa}(2\kappa)}{p^{2\kappa(n-1)}} + O(p^{-M}).$$

Proof. By (3.57) the sum over κ, m in the lemma equals

$$\sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \sum_{0 \le m \le 2\kappa} \Phi_{\kappa,m} + O(p^{-M}).$$

Owing to Lemma 3.5.5 and (3.61), the new sum over κ, m can be expressed as

$$\sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \sum_{0 \le m \le 2\kappa} \frac{1}{p^{mn}} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0, p^m))^2 \\ \gcd(a_1, a_2, p^m) = 1}} S_{\mathbf{a}, p^m} = \sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \frac{\xi_{2\kappa,2\kappa}(2\kappa)}{p^{2\kappa(n-2)}} = \sum_{\kappa \ge 0} \frac{\xi_{2\kappa,2\kappa}(2\kappa)}{p^{2\kappa(n-1)}},$$

thus finishing the proof. □

Recall the definition of the Ramanujan sum in (3.6) and for $\kappa, m \in \mathbb{Z}_{\ge 0}$ with $2\kappa < m$ define

$$\Omega_{\kappa,m} := \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0, p^m))^2 \\ p \nmid \mathbf{a}}} S_{\mathbf{a}, p^m} c_{p^{m-2\kappa}}(-a_1).$$

We then obtain via Lemma 3.5.5 that, in the range $0 \le 2\kappa < m$, we have

$$\frac{\Phi_{\kappa,m}}{p^{2\kappa}} = \left(1 - \frac{1}{p}\right)^{-1} \frac{\Omega_{\kappa,m}}{p^{m(n+1)}}. \tag{3.64}$$

LEMMA 3.5.13. *Keep the assumptions of Theorem 3.1.3. Then for every prime $p \equiv 3 \pmod 4$ and $M \in \mathbb{Z}_{>0}$ the following holds:*

$$\sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \sum_{\substack{0 \le m \le M \\ m = 1 + 2\kappa}} \Phi_{\kappa,m} = \sum_{\kappa \ge 0} \frac{\xi_{2\kappa,1+2\kappa}(1+2\kappa) - \xi_{1+2\kappa,1+2\kappa}(1+2\kappa)}{(1-1/p)p^{(1+2\kappa)(n-1)}}$$
$$- \sum_{\kappa \ge 0} \frac{\xi_{2\kappa,2\kappa}(2\kappa)}{p^{2\kappa(n-1)}} + O(p^{-M}).$$

Proof. First, note that by (3.57) the sum over κ and m in the lemma equals

$$\sum_{\kappa\geq 0} p^{-2\kappa}\Phi_{\kappa,1+2\kappa} + O(p^{-M}).$$

Now using (3.7) we get that $\Omega_{\kappa,m}$ is

$$\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}\Big(p\mathbf{1}_{p|a_1}-1\Big) = p\Big(\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p|a_1,p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}\Big)-\Big(\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}\Big).$$

Writing $a_1 = bp$, we see that $\Omega_{\kappa,m}$ becomes

$$p\left(\sum_{\substack{a_2\in\mathbb{Z}\cap[0,p^m),p\nmid a_2\\ b\in\mathbb{Z}\cap[0,p^{m-1})}} S_{(bp,a_2),p^m}\right) - \left(\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}\right)$$

and the first term equals

$$\begin{aligned} &p\sum_{\substack{a_2\in\mathbb{Z}\cap[0,p^m),p\nmid a_2\\ \mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n}} \mathrm{e}\Big(\frac{a_2 f_2(\mathbf{t})}{p^m}\Big)\sum_{b\in\mathbb{Z}\cap[0,p^{m-1})} \mathrm{e}\Big(\frac{b f_1(\mathbf{t})}{p^{m-1}}\Big)\\ &\quad = p^m \sum_{\substack{a_2\in\mathbb{Z}\cap[0,p^m),p\nmid a_2\\ \mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n, p^{m-1}|f_1(\mathbf{t})}} \mathrm{e}\Big(\frac{a_2 f_2(\mathbf{t})}{p^m}\Big).\end{aligned}$$

The use of the identity (3.7) for the Ramanujan sums appearing in the last line helps in concluding that $\Omega_{\kappa,m}$ equals

$$\begin{aligned} &p^m\left(\Big(\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^m|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} (p-1)p^{m-1}\Big) - \Big(\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{m-1}\|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} p^{m-1}\Big)\right)\\ &\quad - \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}.\end{aligned}$$

We note that $p^{m-1}\|f_2(\mathbf{t})$ holds if and only if $p^{m-1}|f_2(\mathbf{t})$ does and $p^m \mid f_2(\mathbf{t})$ does not hold. Therefore we have

$$\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{m-1}\|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} 1 = \sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{m-1}|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} 1 - \sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{m}|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} 1,$$

which is obviously equal to $p^n\xi_{m-1,m-1}(m-1)-\xi_{m-1,m}(m)$. Hence $\Omega_{\kappa,m}$ becomes

$$\begin{aligned}
&p^m\Big((p-1)p^{m-1}\xi_{m-1,m}(m)-p^{m-1}\Big\{p^n\xi_{m-1,m-1}(m-1)-\xi_{m-1,m}(m)\Big\}\Big)\\
&\quad-\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}}S_{\mathbf{a},p^m}\\
&=p^{2m}\xi_{m-1,m}(m)-p^{2m-1+n}\xi_{m-1,m-1}(m-1)-\sum_{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2,\ p\nmid\mathbf{a}}S_{\mathbf{a},p^m}.
\end{aligned}$$

Thus, by (3.62) we get

$$\begin{aligned}
\Omega_{\kappa,m}=&p^{2m}\xi_{m-1,m}(m)-p^{2m-1+n}\xi_{m-1,m-1}(m-1)\\
&-\xi_{m,m}(m)p^{2m}+p^{2m+n-2}\xi_{m-1,m-1}(m-1)\\
=&p^{2m}(\xi_{m-1,m}(m)-\xi_{m,m}(m))-\xi_{m-1,m-1}(m-1)p^{2m+n-1}(1-p^{-1}).
\end{aligned}$$

Therefore, using (3.64) we infer that $\sum_{\kappa\geq0}\Phi_{\kappa,2\kappa+1}p^{-2\kappa}$ equals

$$\begin{aligned}
\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{1}{p^{m(n+1)}}&(p^{2m}(\xi_{m-1,m}(m)-\xi_{m,m}(m))\\
&-\xi_{m-1,m-1}(m-1)p^{2m+n-1}(1-p^{-1}))
\end{aligned}$$

which is

$$\begin{aligned}
&\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{p^{2m}(\xi_{m-1,m}(m)-\xi_{m,m}(m))}{p^{m(n+1)}}\\
&\qquad-\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{\xi_{m-1,m-1}(m-1)p^{2m+n-1}}{p^{m(n+1)}}\\
&=\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{(\xi_{m-1,m}(m)-\xi_{m,m}(m))}{p^{m(n-1)}}\\
&\qquad-\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{\xi_{m-1,m-1}(m-1)}{p^{(m-1)(n-1)}},
\end{aligned}$$

thus concluding the proof. □

Remark 3.5.14. Taking a step back from the technicalities in the proof, we remark that it is the appearance of the Ramanujan sums that allows us to switch away from the exponential sums in $\Phi_{\kappa,m}$ and into congruential properties of $f_1(\mathbf{t})$ and $f_2(\mathbf{t})$ modulo powers of p.

In order to study the contribution towards $E_\phi(p)$ of the range $\kappa \geq 2+2m$, we shall first need a preparatory lemma.

Lemma 3.5.15. *For each prime $p \equiv 3 \pmod 4$ and all non-negative integers $\kappa \leq -1 + m/2$, the value of $\frac{\Omega_{\kappa,m}}{p^{m(n+1)}}$ equals*

$$\frac{(\xi_{2\kappa,m}(m) - \xi_{1+2\kappa,m}(m))}{p^{m(n-1)}} - \frac{(\xi_{2\kappa,m-1}(m-1) - \xi_{1+2\kappa,m-1}(m-1))}{p^{(m-1)(n-1)}}.$$

Proof. Using (3.7) allows to write $\Omega_{\kappa,m}$ as

$$\begin{aligned}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m} c_{p^{m-2\kappa}}(-a_1) =& p^{m-2\kappa}\Big(\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p^{m-2\kappa}|a_1,p\nmid a_2}} S_{\mathbf{a},p^m}\Big)\\ &- p^{m-2\kappa-1}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p^{m-2\kappa-1}|a_1,p\nmid a_2}} S_{\mathbf{a},p^m}.\end{aligned}$$

Writing $a_1 = p^{m-2\kappa}b$ shows

$$\begin{aligned}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p^{m-2\kappa}|a_1,p\nmid a_2}} S_{\mathbf{a},p^m} &= \sum_{\substack{a_2\in(\mathbb{Z}\cap[0,p^m),p\nmid a_2\\ \mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n}} \mathrm{e}\Big(\frac{a_2 f_2(\mathbf{t})}{p^m}\Big)\sum_{b\in\mathbb{Z}\cap[0,p^{2\kappa})}\mathrm{e}\Big(\frac{b f_1(\mathbf{t})}{p^{2\kappa}}\Big)\\ &= p^{2\kappa}\sum_{\substack{a_2\in(\mathbb{Z}\cap[0,p^m)\\ \mathbf{t}\in(\mathbb{Z}/p^m\mathbb{Z})^n\\ p^{2\kappa}|f_1(\mathbf{t}),\ p\nmid a_2}}\mathrm{e}\Big(\frac{a_2 f_2(\mathbf{t})}{p^m}\Big).\end{aligned}$$

Recalling (3.6) and using (3.7), this can now be written as

$$\begin{aligned}p^{2\kappa}\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{2\kappa}|f_1(\mathbf{t})}} c_{p^m}(f_2(\mathbf{t})) =& p^{2\kappa+m}\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{2\kappa}|f_1(\mathbf{t}),p^m|f_2(\mathbf{t})}} 1\\ &- p^{2\kappa+m-1}\sum_{\substack{\mathbf{t}\in(\mathbb{Z}/p^m\mathbb{Z})^n\\ p^{2\kappa}|f_1(\mathbf{t}),p^{m-1}|f_2(\mathbf{t})}} 1\\ =& p^{2\kappa+m}\xi_{2\kappa,m}(m) - p^{n+2\kappa+m-1}\xi_{2\kappa,m-1}(m-1).\end{aligned}$$

A completely analogous argument shows

$$\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p^{m-2\kappa-1}|a_1,p\nmid a_2}} S_{\mathbf{a},p^m} = p^{1+2\kappa+m}\xi_{1+2\kappa,m}(m) - p^{n+2\kappa+m}\xi_{1+2\kappa,m-1}(m-1).$$

Therefore, we see that $\Omega_{\kappa,m}$ is

$$\begin{aligned} &p^{2m}(\xi_{2\kappa,m}(m) - p^{n-1}\xi_{2\kappa,m-1}(m-1)) \\ &\qquad - p^{2m-1}(p\xi_{1+2\kappa,m}(m) - p^n\xi_{1+2\kappa,m-1}(m-1)) \\ &= p^{2m}(\xi_{2\kappa,m}(m) - \xi_{1+2\kappa,m}(m)) \\ &\qquad - p^{2m-1+n}(\xi_{2\kappa,m-1}(m-1) - \xi_{1+2\kappa,m-1}(m-1)), \end{aligned}$$

thus concluding the proof. □

Lemma 3.5.16. *Under the assumptions of Theorem 3.1.3, fix any prime $p \equiv 3 \pmod 4$. Then for all $M \in \mathbb{Z}_{>0}$ we have equality of*

$$\sum_{\substack{0\le\kappa\le M/2-1\\ 2+2\kappa\le m\le M}} \frac{\Phi_{\kappa,m}}{p^{2\kappa}}$$

and

$$\begin{aligned} &\left(1-\frac{1}{p}\right)^{-1}\frac{\#\left\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\right\}}{p^{M(n-1)}} \\ &-\left(1-\frac{1}{p}\right)^{-1}\sum_{0\le\kappa\le -1+M/2}\frac{(\xi_{2\kappa,1+2\kappa}(1+2\kappa)-\xi_{1+2\kappa,1+2\kappa}(1+2\kappa))}{p^{(1+2\kappa)(n-1)}} \end{aligned}$$

up to an error term that is $O_p(p^{-M})$.

Proof. From (3.64) and Lemma 3.5.15 we get that the sum over κ, m in our lemma equals

$$\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{0\le\kappa\le -1+M/2\\ 2+2\kappa\le m\le M}}\left(\frac{(\xi_{2\kappa,m}(m)-\xi_{1+2\kappa,m}(m))}{p^{m(n-1)}} - \frac{(\xi_{2\kappa,m-1}(m-1)-\xi_{1+2\kappa,m-1}(m-1))}{p^{(m-1)(n-1)}}\right).$$

Noting that for fixed κ the sum over m is telescopic, we can rewrite the last expression as

$$\left(1-\frac{1}{p}\right)^{-1}\sum_{0\le\kappa\le -1+M/2}\left(\frac{(\xi_{2\kappa,M}(M)-\xi_{1+2\kappa,M}(M))}{p^{M(n-1)}}\right.$$
$$\left.-\frac{(\xi_{2\kappa,1+2\kappa}(1+2\kappa)-\xi_{1+2\kappa,1+2\kappa}(1+2\kappa))}{p^{(1+2\kappa)(n-1)}}\right).$$

Let us now focus on the first part of the sum. Definition (3.60) makes immediately apparent that $\sum_{0\le\kappa\le -1+M/2}(\xi_{2\kappa,M}(M)-\xi_{1+2\kappa,M}(M))$ equals

$$\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\cap[0,M-2]\big\}.$$

The contribution of those $\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n$ with $v_p(f_1(\mathbf{t}))\ge M-1$ can be controlled by using Lemma 3.5.10 with $m_1=M-1$ and $m_2=M$. We then obtain

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\cap[0,M-2]\big\}}{p^{M(n-1)}}$$
$$=\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\big\}}{p^{M(n-1)}}+O_p(p^{-M}),$$

thereby proving that the sum over κ, m in our lemma is

$$\left(1-\frac{1}{p}\right)^{-1}\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\big\}}{p^{M(n-1)}}$$
$$-\left(1-\frac{1}{p}\right)^{-1}\sum_{0\le\kappa\le -1+M/2}\frac{(\xi_{2\kappa,1+2\kappa}(1+2\kappa)-\xi_{1+2\kappa,1+2\kappa}(1+2\kappa))}{p^{(1+2\kappa)(n-1)}}$$

up to an error term of $O_p(p^{-M})$. □

Lemma 3.5.17. *Under the assumptions of Theorem 3.1.3, fix any prime $p\equiv 3\,(\mathrm{mod}\ 4)$. Then for all $M\in\mathbb{Z}_{>0}$ we have*

$$\left(1-\frac{1}{p}\right)^{-1}\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\big\}}{p^{M(n-1)}}=E_\Phi(p)$$

up to an error term of $O_p(p^{-M})$

Proof. Putting together Lemmas 3.5.12, 3.5.13 and 3.5.16 and taking into account the occurence of many cancellations, we obtain the equality of $\sum_{\kappa\geq 0}\frac{1}{p^{2\kappa}}\sum_{0\leq m\leq M}\Phi_{\kappa,m}$ and

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\big\}}{(1-1/p)p^{M(n-1)}}+\mathcal{H}+O_p(p^{-M}),$$

where

$$\mathcal{H}:=\sum_{\kappa>-1+M/2}\frac{(\xi_{2\kappa,1+2\kappa}(1+2\kappa)-\xi_{1+2\kappa,1+2\kappa}(1+2\kappa))}{(1-1/p)p^{(1+2\kappa)(n-1)}}$$

comes from the part of the equation of Lemma 3.5.13 that is not cancelled out by any other terms. Next, note that Lemma 3.5.10 provides us with

$$\frac{|\xi_{2\kappa,1+2\kappa}(1+2\kappa)|+|\xi_{1+2\kappa,1+2\kappa}(1+2\kappa)|}{p^{(1+2\kappa)(n-1)}}\ll_p p^{-2\kappa}$$

and therefore $\mathcal{H}=O_p(p^{-M})$. Finally, (3.57) allows to complete the sum in the statement of the current lemma at the cost of an error term of size $O_p(p^{-M})$. □

Proof of Proposition 3.5.11. By Lemma 3.5.17 it is obvious that the sequence

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^N))^n : f_1(\mathbf{t})\neq 0, p^N \mid f_2(\mathbf{t}), x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \text{ has a } \mathbb{Q}_p\text{-point}\big\}}{p^{N(n-1)}}$$

has a limit for $N\to\infty$, because for a non-zero integer m, the curve $x_0^2+x_1^2=mx_2^2$ has a $\mathbb{Q}_p$-point if and only if $v_p(m)$ is even. Furthermore, if $f_1(\mathbf{t})$ vanishes then p^N divides $f_1(\mathbf{t})$ and therefore the bound (3.63) shows that the condition $f_1(\mathbf{t})\neq 0$ can be removed from the numerator of the limit above. This proves the existence of the limit ℓ_p and it is clear that the equality $E_\Phi(p)=(1-1/p)^{-1}\ell_p$ follows instantly by Lemma 3.5.17. □

3.5.3 Local density at the prime 2

We begin by stating the main result of this section.

Proposition 3.5.18. *Under the assumptions of Theorem 3.1.3, the sequence*

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,2^N))^n : f_2(\mathbf{t})\equiv 0\pmod{2^N}, x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \textit{ has a } \mathbb{Q}_2\textit{-point}\big\}}{2^{N(n-1)}}$$

has a limit for $N \to \infty$ which we call ℓ_2 and we have $\ell_2 = E_\phi(2)$.

The proof of Proposition 3.5.18 will follow steps somewhat similar to those in the proof of Proposition 3.5.11. However, there will be now four cases rather than merely three, the reason being the presence of the term $\mathbf{1}_{v_2(b_1)\geq \varrho-t-2}$ in the definition of $E_\phi(2)$ in (3.56). The four cases will be $\varrho \leq t$, $\varrho = t+1$, $\varrho = t+2$, and $\varrho \geq t+3$ that will be dealt with in Lemmas 3.5.19, 3.5.20, 3.5.21 and 3.5.22 respectively. There are further minor differences between the proofs of Proposition 3.5.11 and Proposition 3.5.18. They are related to the difference between the two formulas $\ell_p = (1-1/p)E_\phi(p)$ and $\ell_2 = E_\phi(2)$.

Recall the definition of $S_{\mathbf{a},q}$ in (3.13) and that of $\xi_{i,j}(m)$ in (3.60).

LEMMA 3.5.19. *Under the assumptions of Theorem 3.1.3 the following two series converge absolutely:*

$$\sum_{t=0}^{\infty}\sum_{\varrho=0}^{t}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^\varrho))^2\\ \gcd(b_1,b_2,2^\varrho)=1}} S_{\mathbf{b},2^\varrho}\,\mathrm{e}(-b_1 2^{t-\varrho})\mathbf{1}_{v_2(b_1)\geq\varrho-t-2},$$

and

$$\sum_{t=0}^{\infty}\frac{\xi_{t,t}(t)}{2^{t(n-1)}}.$$

In addition, they are equal.

Proof. The absolute convergence of the former sum is a direct consequence of (3.28), while the absolutely convergence of the latter sum is a consequence of (3.63). To verify the claimed equality observe that the first sum in the lemma can clearly be written as

$$\sum_{t\geq 0}\frac{1}{2^t}\sum_{0\leq\varrho\leq t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^\varrho))^2\\ \gcd(b_1,b_2,2^\varrho)=1}} S_{\mathbf{b},2^\varrho}$$

and by (3.61) the new sum over ϱ equals $\xi_{t,t}(t)2^{-t(n-2)}$. □

LEMMA 3.5.20. *Under the assumptions of Theorem 3.1.3 all series over $t \geq 0$ in the following two expressions converge absolutely:*

$$\sum_{t\geq 0}\frac{1}{2^t}\frac{1}{2^{(t+1)n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{t+1}))^2\\ \gcd(b_1,b_2,2)=1}} S_{\mathbf{b},2^{t+1}}\,\mathrm{e}(-b_1 2^{-1}),$$

and

$$2\sum_{t\ge 0}\frac{(\xi_{t,t+1}(t+1)-\xi_{t+1,t+1}(t+1))}{2^{(1+t)(n-1)}}-\sum_{t\ge 0}\frac{\xi_{t,t}(t)}{2^{t(n-1)}}.$$

In addition, the two expressions are equal.

Proof. The absolute convergence follows from taking $M=t$, $m_2=t$, $m_1=t-1$ in Lemma 3.5.10, as well as (3.28) and (3.63). Furthermore, the sum over $\mathbf{b}$ in the lemma equals

$$\sum_{\substack{b_2\in\mathbb{Z}\cap[0,2^{t+1})\\ \mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n}}\mathrm{e}\left(\frac{b_2f_2(\mathbf{x})}{2^{t+1}}\right)\sum_{\substack{b_1\in\mathbb{Z}\cap[0,2^{t+1})\\ 2\nmid\mathbf{b}}}\mathrm{e}(-b_1/2)\,\mathrm{e}\left(\frac{b_1f_1(\mathbf{x})}{2^{t+1}}\right).$$

The contribution of the even values of b_1 is the following (after writing $b_1=2c$),

$$\mathbf{1}_{2\nmid b_2}\sum_{c\in\mathbb{Z}\cap[0,2^t)}\mathrm{e}\left(\frac{cf_1(\mathbf{x})}{2^t}\right)=2^t\mathbf{1}_{2\nmid b_2}\mathbf{1}_{2^t\mid f_1(\mathbf{x})}$$

and the contribution of the odd values equals

$$-\mathrm{e}\left(\frac{f_1(\mathbf{x})}{2^{t+1}}\right)\sum_{c\in\mathbb{Z}\cap[0,2^t)}\mathrm{e}\left(\frac{cf_1(\mathbf{x})}{2^t}\right)=-\mathrm{e}\left(\frac{f_1(\mathbf{x})}{2^{t+1}}\right)2^t\mathbf{1}_{2^t\mid f_1(\mathbf{x})}$$

after writing $b_1=2c+1$. Recalling (3.6), we infer that the sum over $\mathbf{b}$ in the lemma is

$$2^t\sum_{\substack{b_2\in\mathbb{Z}\cap[0,2^{t+1})\\ \mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n\\ 2^t\mid f_1(\mathbf{x})}}\mathrm{e}\left(\frac{b_2f_2(\mathbf{x})}{2^{t+1}}\right)\left(\mathbf{1}_{2\nmid b_2}-\mathrm{e}\left(\frac{f_1(\mathbf{x})2^{-t}}{2}\right)\right),$$

which is plainly

$$2^t\left(\sum_{\substack{\mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n\\ 2^t\mid f_1(\mathbf{x})}}c_{2^{t+1}}(f_2(\mathbf{x}))\right)-2^{1+2t}\left(\sum_{\substack{\mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n\\ 2^{t+1}\mid f_1(\mathbf{x}),2^{t+1}\mid f_2(\mathbf{x})}}1\right)$$
$$+2^{1+2t}\left(\sum_{\substack{\mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n\\ v_2(f_1(\mathbf{x}))=t,2^{t+1}\mid f_2(\mathbf{x})}}1\right).$$

Using (3.7) to simplify the first sum over $\mathbf{x}$ shows that the left side of the equation in the current lemma is

$$\sum_{t\geq 0}\frac{1}{2^t}\frac{1}{2^{(t+1)n}}(2^{2+2t}\xi_{t,t+1}(t+1)-2^{2+2t}\xi_{t+1,t+1}(t+1)-2^{n+2t}\xi_{t,t}(t)),$$

which concludes the proof. □

Write $\lambda_t(M)$ for

$$\#\big\{\mathbf{x}\in\big(\mathbb{Z}\cap[0,2^M)\big)^n : v_2(f_1(\mathbf{x}))=t, 2^M \mid f_2(\mathbf{x}), f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1 \,(\mathrm{mod}\ 4)\big\},$$

where for any integer n we write n_{odd} for $n\cdot 2^{-v_2(n)}$.

LEMMA 3.5.21. *Under the assumptions of Theorem 3.1.3 all series over t in the following two quantities converge absolutely:*

$$\sum_{t\geq 0}\frac{1}{2^t}\frac{1}{2^{n(t+2)}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{t+2}))^2\\ \gcd(b_1,b_2,2^{t+2})=1}} S_{\mathbf{b},2^{t+2}}\,\mathrm{e}(-b_1/4),$$

$$4\sum_{t\geq 0}\frac{\lambda_t(t+2)}{2^{(n-1)(t+2)}}-2\sum_{t\geq 0}\frac{(\xi_{t,t+1}(t+1)-\xi_{t+1,t+1}(t+1))}{2^{(n-1)(t+1)}}.$$

Furthermore, the two quantities are equal.

Proof. The first series and the second term in the second series can be proven to converge absolutely in the same way as in the proof of Lemma 3.5.20. To prove absolute convergence for the first term of the second series we note that we may bound $\lambda_t(t+2)\leq\xi_{t,t+2}(t+2)$ and hence by Lemma 3.5.10 we have $\lambda_t(t+2)\ll 2^{nt+2n-2t}$, which is sufficient.

Let us now proceed with the proof of the claimed equality. The sum over $\mathbf{b}$ is

$$\sum_{\substack{b_2\in\mathbb{Z}\cap[0,2^{t+2})\\ \mathbf{x}\in\mathbb{Z}\cap[0,2^{t+2})^n}}\mathrm{e}\left(\frac{b_2f_2(\mathbf{x})}{2^{t+2}}\right)\sum_{\substack{b_1\in\mathbb{Z}\cap[0,2^{t+2})\\ 2\nmid\mathbf{b}}}\mathrm{e}(-b_1/4)\,\mathrm{e}\left(\frac{b_1f_1(\mathbf{x})}{2^{t+2}}\right).$$

The new sum over b_1 can be written as follows (after writing $b_1=4y+j$),

$$\sum_{\substack{j\in\mathbb{Z}\cap[0,4)\\ 2\mid j\Rightarrow 2\nmid b_2}}\mathrm{e}(-j/4)\,\mathrm{e}\Big(\frac{jf_1(\mathbf{x})}{2^{t+2}}\Big)\sum_{y\in\mathbb{Z}\cap[0,2^t)}\mathrm{e}\Big(\frac{yf_1(\mathbf{x})}{2^t}\Big)$$

which is equal to

$$2^t \mathbf{1}_{2^t | f_1(\mathbf{x})} \sum_{\substack{j \in \mathbb{Z} \cap [0,4) \\ 2|j \Rightarrow 2 \nmid b_2}} \mathrm{e}(-j/4)\, \mathrm{e}\Big(\frac{j f_1(\mathbf{x})}{2^{t+2}}\Big).$$

A moment's thought allows to verify the following identity for any integer c:

$$\sum_{\substack{j \in \mathbb{Z} \cap [0,4) \\ 2|j \Rightarrow 2 \nmid b_2}} \mathrm{e}(jc/4) = 2(\mathbf{1}_{2 \nmid b_2} + e(c/4))\mathbf{1}_{2|c}.$$

Using this for $c = f_1(\mathbf{x})2^{-t} - 1$ provides us with the equality of the sum over b_1 with

$$2^{t+1} \mathbf{1}_{v_2(f_1(\mathbf{x}))=t} (\mathbf{1}_{2 \nmid b_2} + \mathrm{e}((f_1(\mathbf{x})2^{-t} - 1)/4)).$$

Hence the sum over $\mathbf{b}$ in the lemma is

$$2^{t+1} \sum_{\substack{b_2 \in \mathbb{Z} \cap [0, 2^{t+2}) \\ \mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n, v_2(f_1(\mathbf{x}))=t}} \mathrm{e}\Big(\frac{b_2 f_2(\mathbf{x})}{2^{t+2}}\Big)\Big(\mathbf{1}_{2 \nmid b_2} + \mathrm{e}((f_1(\mathbf{x})2^{-t} - 1)/4)\Big),$$

which is

$$2^{t+1} \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t}} c_{2^{t+2}}(f_2(\mathbf{x})) + 2^{3+2t} \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t, 2^{t+2} | f_2(\mathbf{x})}} \mathrm{e}((f_1(\mathbf{x})2^{-t} - 1)/4).$$

Furthermore we have

$$\sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t \\ 2^{t+2} | f_2(\mathbf{x})}} \mathrm{e}((f_1(\mathbf{x})2^{-t} - 1)/4) = \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t, 2^{t+2} | f_2(\mathbf{x}) \\ f_1(\mathbf{x})_{\mathrm{odd}} \equiv 1 \pmod 4}} 1 - \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t, 2^{t+2} | f_2(\mathbf{x}) \\ f_1(\mathbf{x})_{\mathrm{odd}} \equiv 3 \pmod 4}} 1,$$

and, since $v_2(f_1(\mathbf{x})) = t$ implies $f_1(\mathbf{x})_{\mathrm{odd}} = f_1(\mathbf{x})2^{-t}$, this can now be written as

$$2 \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t \\ 2^{t+2} | f_2(\mathbf{x}) \\ f_1(\mathbf{x})_{\mathrm{odd}} \equiv 1 \pmod 4}} 1 - \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t \\ 2^{t+2} | f_2(\mathbf{x})}} 1 = 2\lambda_t(t+2) - (\xi_{t,t+2}(t+2) - \xi_{t+1,t+2}(t+2)).$$

Hence, the sum over $\mathbf{b}$ in the lemma is

$$2^{t+1}\sum_{\substack{\mathbf{x}\in\mathbb{Z}\cap[0,2^{t+2})^n\\ v_2(f_1(\mathbf{x}))=t}} c_{2^{t+2}}(f_2(\mathbf{x}))+2^{3+2t}\Big(2\lambda_t(t+2)-(\xi_{t,t+2}(t+2)-\xi_{t+1,t+2}(t+2))\Big).$$

Utilising (3.7) to evaluate $c_{2^{t+2}}(f_2(\mathbf{x}))$ concludes the proof. □

The next lemma is the last one in the established line of similar results.

LEMMA 3.5.22. *Under the assumptions of Theorem 3.1.3 both series over t in the following expression converge absolutely:*

$$\sum_{t\geq 0}\frac{\lambda_t(t+2)}{2^{(t+2)(n-1)}}+\frac{1}{4}\sum_{\substack{t\geq 0\\ \varrho\geq t+3}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^\varrho))^2\\ 2^{\varrho-t-2}|b_1,2\nmid b_2}} S_{\mathbf{b},2^\varrho}\,\mathrm{e}(-b_1 2^{t-\varrho}).$$

Furthermore, the limit

$$\lim_{M\to\infty}\frac{\#\left\{\mathbf{x}\in\left(\mathbb{Z}\cap[0,2^M)\right)^n : f_2(\mathbf{x})\equiv 0\left(\mathrm{mod}\ 2^M\right), f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1\,(\mathrm{mod}\ 4)\right\}}{2^{M(n-1)}}$$

exists and is equal to the previous expression.

Proof. The proof of the absolute convergence is similar to that in the proof of Lemma 3.5.21, thus we shall next concentrate on showing the existence of the limit in the lemma. Writing $b_1=2^{\varrho-t-2}(4y+j)$ and using (3.7), we see that the sum over $\mathbf{b}$ becomes

$$\sum_{\mathbf{x}\in(\mathbb{Z}\cap[0,2^\varrho))^n} c_{2^\varrho}(f_2(\mathbf{x}))\sum_{j\in\mathbb{Z}\cap[0,4)}\mathrm{e}(-j/4)\,\mathrm{e}\Big(\frac{jf_1(\mathbf{x})}{2^{t+2}}\Big)\sum_{y\in\mathbb{Z}\cap[0,2^t)}\mathrm{e}\Big(\frac{yf_1(\mathbf{x})}{2^t}\Big),$$

which equals

$$2^{t+\varrho}\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\cap[0,2^\varrho))^n\\ 2^t|f_1(\mathbf{x})}}\Big(\mathbf{1}_{2^\varrho|f_2(\mathbf{x})}-\frac{\mathbf{1}_{2^{\varrho-1}|f_2(\mathbf{x})}}{2}\Big)\sum_{j\in\mathbb{Z}\cap[0,4)}\mathrm{e}(-j/4)\,\mathrm{e}\Big(\frac{jf_1(\mathbf{x})}{2^{t+2}}\Big).$$

Noting that the sum over j equals 4 when $4\mid f_1(\mathbf{x})2^{-t}-1$ holds, and it otherwise vanishes, we obtain

$$2^{t+\varrho+2}\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\cap[0,2^\varrho))^n\\ 2^t|f_1(\mathbf{x}),4|f_1(\mathbf{x})2^{-t}-1}}\Big(\mathbf{1}_{2^\varrho|f_2(\mathbf{x})}-\frac{\mathbf{1}_{2^{\varrho-1}|f_2(\mathbf{x})}}{2}\Big),$$

which can be written as

$$2^{t+\varrho+2}\Bigg(\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\cap[0,2^{\varrho}))^n\\ v_2(f_1(\mathbf{x}))=t,2^{\varrho}\mid f_2(\mathbf{x})\\ f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1(\mathrm{mod}\ 4)}}1\Bigg)-2^{t+\varrho+1+n}\Bigg(\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\cap[0,2^{\varrho-1}))^n\\ v_2(f_1(\mathbf{x}))=t,2^{\varrho-1}\mid f_2(\mathbf{x})\\ f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1(\mathrm{mod}\ 4)}}1\Bigg).$$

Therefore, whenever M is an integer with $M > t+3$, we have

$$\sum_{\substack{t\geq 0\\ t+3\leq\varrho\leq M}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{\varrho}))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}}S_{\mathbf{b},2^{\varrho}}\,\mathrm{e}(-b_1 2^{t-\varrho})$$
$$=4\sum_{t\geq 0}\sum_{\varrho=t+3}^{M}\left(\frac{\lambda_t(\varrho)}{2^{\varrho(n-1)}}-\frac{\lambda_t(\varrho-1)}{2^{(\varrho-1)(n-1)}}\right).$$

The sum over ϱ is telescopic, thus we get

$$\sum_{\substack{t\geq 0\\ t+3\leq\varrho\leq M}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{\varrho}))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}}S_{\mathbf{b},2^{\varrho}}\,\mathrm{e}(-b_1 2^{t-\varrho})=4\left(\frac{\lambda_t(M)}{2^{M(n-1)}}-\frac{\lambda_t(t+2)}{2^{(t+2)(n-1)}}\right).$$

Using the bound (3.28) we obtain

$$\sum_{t\geq 0}\frac{1}{2^t}\sum_{\varrho>M}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{\varrho}))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}}|S_{\mathbf{b},2^{\varrho}}\,\mathrm{e}(-b_1 2^{t-\varrho})|\ll\sum_{t\geq 0}\frac{1}{2^t}\sum_{\varrho>M}\frac{1}{2^{\varrho n}}2^{\rho(n-3)}$$
$$\ll 2^{-M},$$

and therefore also

$$\sum_{\substack{t\geq 0\\ \varrho\geq t+3}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{\varrho}))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}}S_{\mathbf{b},2^{\varrho}}\,\mathrm{e}(-b_1 2^{t-\varrho})-4\sum_{t\geq 0}\left(\frac{\lambda_t(M)}{2^{M(n-1)}}-\frac{\lambda_t(t+2)}{2^{(t+2)(n-1)}}\right)$$

is $O(2^{-M})$. Taking $M\to\infty$ and noting

$$\sum_{t\geq 0}\frac{\lambda_t(M)}{2^{M(n-1)}}=\frac{\#\big\{\mathbf{x}\in\big(\mathbb{Z}\cap[0,2^M)\big)^n : 2^M\mid f_2(\mathbf{x}), f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1\,(\mathrm{mod}\ 4)\big\}}{2^{M(n-1)}}$$

shows that the limit

$$\lim_{M\to\infty}\frac{\#\big\{\mathbf{x}\in\big(\mathbb{Z}\cap[0,2^M)\big)^n : 2^M\mid f_2(\mathbf{x}), f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1\,(\mathrm{mod}\ 4)\big\}}{2^{M(n-1)}}$$

exists and equals

$$\sum_{t\geq 0}\frac{\lambda_t(t+2)}{2^{(t+2)(n-1)}}+\frac{1}{4}\sum_{\substack{t\geq 0\\ \varrho\geq t+3}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^\varrho))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}} S_{\mathbf{b},2^\varrho}\,\mathrm{e}(-b_1 2^{t-\varrho}).$$

This concludes the proof. □

Proof of Proposition 3.5.18. First, the contribution of those $\mathbf{t}$ with $f_2(\mathbf{t})$ being zero in the quantity inside the limit defining ℓ_2 in Proposition 3.5.18 can be dealt with in an identical manner as in our proof of Proposition 3.5.11.

Using Hilbert symbols (see, for example, [Ser73, Ch.III,Th.1]) one can obtain that for an integer m the curve $x_0^2+x_1^2=mx_2^2$ has a point over $\mathbb{Q}_2$ if and only if the odd part of m is $1\,(\mathrm{mod}\ 4)$. Hence the limit ℓ_2 in Proposition 3.5.18 coincides with the limit in Lemma 3.5.22, thus ℓ_2 exists. Finally, to prove $E_\phi(2)=\ell_2$, recall that $E_\phi(2)$ can be represented as the sum over t,ϱ in (3.56) and combine the equalities proved in Lemmas 3.5.19, 3.5.20, 3.5.21 and 3.5.22. □

3.5.4 Concluding steps

For every prime p we define

$$\tau_p:=\frac{(1-\frac{1}{p^{n-d}})}{(1-\frac{1}{p})}\lim_{N\to\infty}L_N$$

where L_N is equal

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^N))^n : p^N\mid f_2(\mathbf{t}), x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \text{ has a } \mathbb{Q}_p\text{-point}\big\}}{p^{N(n-1)}}.$$

This is well defined because for $p\equiv 1\,(\mathrm{mod}\ 4)$ the limit coincides with $\tau_{f_2}(p)$ which was introduced in (3.50), and for $p\not\equiv 1\,(\mathrm{mod}\ 4)$ the limit coincides with ℓ_p and ℓ_2 from Propositions 3.5.11 and 3.5.18 respectively. The definition of τ_p is motivated by the construction of the Tamagawa measure by Loughran in [Lou13, §5.7.2]. It is useful to recall that if one were counting $\mathbb{Q}$-rational points on the hypersurface $f_2=0$ then the corresponding Peyre constant would involve a p-adic density that is the

same as the number τ_p except for the condition on $\mathbb{Q}_p$-solubility, see [PT01, Cor.3.5]. For $s \in \mathbb{C}$ with $\Re(s) > 1$ let

$$L(s) := \sqrt{\zeta(s)} \tag{3.65}$$

denote the p-adic factor of $L(s)$ by $L_p(s)$ and write λ_p for $L_p(1)$, i.e.

$$\lambda_p := \left(1 - \frac{1}{p}\right)^{-1/2}.$$

Recall the definition of the real density $\mathfrak{J}$ in (3.33) and that d denotes the degrees of f_1 and f_2 (which are equal and even).

THEOREM 3.5.23. *Keep the assumptions of Theorem 3.1.3.*

1. *If ϕ has a smooth fibre with a $\mathbb{Q}$-point then the constant c_ϕ in Theorem 3.1.3 is strictly positive.*
2. *The infinite product $\prod_p \frac{\tau_p}{\lambda_p}$ taken over all non-archimedean places converges.*
3. *The constant c_ϕ in Theorem 3.1.3 satisfies*

$$c_\phi = \frac{\frac{1}{\sqrt{d}}\mathfrak{J}\prod_p \frac{\tau_p}{\lambda_p}}{\sqrt{\pi}}.$$

REMARK 3.5.24. Recalling that $\sqrt{\pi}$ is the value of the Euler Gamma function at $1/2$ and noting that

$$1 = \lim_{s \to 1_+} (s-1)^{1/2} L(s)$$

allows for a comparison of Theorem 3.5.23 with the case of [Lou13, Th. 5.15] that corresponds to

$$\rho_{\mathcal{B}}(X) = \frac{1}{2}.$$

Proof of Theorem 3.5.23. To prove *(1)* observe that due to (3.40), it suffices to show that if ϕ has a smooth fibre with a $\mathbb{Q}$-point then

$$\mathfrak{J} > 0 \text{ and } \mathbb{L}_\phi > 0.$$

For the former part, we point the reader to the definition of $\mathfrak{J}$ in (3.33). One should first notice that if $\mathcal{V} \subset [-1,1]^n$ is an area without zeroes of f_2, then the integral

$$\int_{\Gamma \in \mathbb{R}} \int_{\mathbf{t} \in \mathcal{V}} e(\Gamma f_2(\mathbf{t})) \mathrm{d}\mathbf{t} \mathrm{d}\Gamma$$

vanishes.

Let us write $\mathcal{A} := \{\mathbf{t} \in (-1,1)^n \mid f_1(\mathbf{t}) > 0\}$. Then the closure of $\mathcal{A}$ is the region of integration that appears in $\mathfrak{J}$. Since the boundary has measure zero, integrating over $\mathcal{A}$ gives the same result. Divide $\mathcal{A}$ up into sufficiently small boxes with sides parallel to the coordinate axes, not necessarily finite in number and not necessarily of equal sizes. Since we already know that the integral $\mathfrak{J}$ converges to a finite value, this value is equal to the possibly infinite sum of integrals over these boxes.

It is proved in [Bir62, §6], that if $\mathcal{B} \subset (-1,1)^n$ is a box with sides parallel to the coordinate axes and the hypersurface $f_2 = 0$ has a non-singular real point inside $\mathcal{B}$ then the corresponding integral

$$\int_{\Gamma\in\mathbb{R}} \int_{\mathbf{t}\in\mathcal{B}} \mathrm{e}(\Gamma f_2(\mathbf{t}))\mathrm{d}\mathbf{t}\mathrm{d}\Gamma$$

is positive. In our case, every real zero of f_2 is non-singular by assumption. Combined with the vanishing mentioned above, the integral over any box in the subdivision of $\mathcal{A}$ is non-negative, so we only need to prove the existence of one box containing a real zero of f_2.

Now, in *(1)* it is assumed that ϕ has a smooth fibre with a $\mathbb{Q}$-point. This means that there exists a point $\mathbf{t} \in \mathbb{P}^{n-1}(\mathbb{Q})$ such that for any representative $\mathbf{t}_0 \in \mathbb{Q}^n$ we have $f_2(\mathbf{t}_0) = 0$, and moreover the curve $x_0^2 + x_1^2 = f_1(\mathbf{t}_0)x_2^2$ is smooth and has a $\mathbb{Q}$-point, hence in particular an $\mathbb{R}$-point. Therefore we have $f_1(\mathbf{t}_0) > 0$. Choosing such $\mathbf{t}_0$ inside $(-1,1)^n$, we get the desired existence of $\mathbf{t}_0 \in \mathcal{A}$ satisfying $f_2(\mathbf{t}_0) = 0$. Subsequently we find a box $\mathcal{B} \subset \mathcal{A}$ with sides parallel to the coordinate axes containing $\mathbf{t}_0$. Therefore the integral over this particular box is positive, and in conclusion $\mathfrak{J}$ is positive.

To prove $\mathbb{L}_\phi > 0$, we invoke Lemma 3.5.9 to see that it is enough to show

$$\begin{aligned} &E_\phi(2) > 0, \text{ and} \\ &p \equiv 1 \,(\mathrm{mod}\ 4) \Rightarrow \tau_{f_2}(p) > 0, \text{ and} \\ &p \equiv 3 \,(\mathrm{mod}\ 4) \Rightarrow E_\phi(p) > 0. \end{aligned} \tag{3.66}$$

For this, choose a representative $\mathbf{t}_0$ in $\mathbb{Z}^n_{\mathrm{prim}}$ (rather than in $(-1,1)^n$ as in the previous paragraph) and note that for every prime p the point $\mathbf{t}_0$ can be viewed as a smooth $\mathbb{Q}_p$-point on the hypersurface $f_2 = 0$ and such that the curve $x_0^2 + x_1^2 = f_1(\mathbf{t}_0)x_2^2$ has a $\mathbb{Q}_p$-point. For $p \equiv 1 \,(\mathrm{mod}\ 4)$ this forces no condition on $f_1(\mathbf{t}_0)$, thus $\tau_{f_2}(p) > 0$ because, as mentioned

in [Bir62, §7], one can use Hensel's lemma to prove that if $f_2 = 0$ has a smooth $\mathbb{Q}_p$-point then the analogous p-adic density is strictly positive. If $p \equiv 3 \pmod 4$ or if $p = 2$ then the existence of such a $\mathbf{t}_0$ can be used with Hensel's lemma to prove that the quantities ℓ_2 and ℓ_p (defined in Propositions 3.5.11 and 3.5.18 respectively) are strictly positive. The equalities $E_\phi(p) = \ell_p/(1-1/p)$ and $E_\phi(2) = \ell_2$ (proved in Propositions 3.5.11 and 3.5.18) then show the validity of (3.66), which concludes the proof of *(1)*.

Let us now commence the proof of *(2)*. Denoting the limit in the definition of τ_p by ℓ_p we see

$$\begin{aligned}\lim_{t\to\infty}\prod_{p\le t}\frac{\tau_p}{\lambda_p} &= \lim_{t\to\infty}\prod_{p\le t}\frac{(1-\frac{1}{p^{n-d}})}{(1-\frac{1}{p})}\ell_p\Big(1-\frac{1}{p}\Big)^{1/2}\\ &= \frac{\ell_2 2^{1/2}}{\zeta(n-d)}\lim_{t\to\infty}\prod_{2\neq p\le t}\frac{\ell_p}{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}\left(\frac{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}{(1-\frac{\mathbf{1}_{p\equiv 1(\mathrm{mod}\ 4)}}{p})}\right)^{1/2}.\end{aligned}$$

We now let χ stand for the non-trivial Dirichlet character (mod 4) to obtain

$$\prod_{p\le t}\frac{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}{(1-\frac{\mathbf{1}_{p\equiv 1(\mathrm{mod}\ 4)}}{p})} = \left(\prod_{p\le t}\frac{1}{1-\frac{\chi(p)}{p}}\right)\prod_{\substack{p\le t\\ p\equiv 3(\mathrm{mod}\ 4)}}\Big(1-\frac{1}{p^2}\Big).$$

Applying the Leibniz formula for π, or in other words, that the Euler product for the Dirichlet series $L(\chi,s)$ of χ converges to $\pi/4$ for $s=1$, we get

$$\lim_{t\to\infty}\prod_{p\le t}\left(\frac{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}{(1-\frac{\mathbf{1}_{p\equiv 1(\mathrm{mod}\ 4)}}{p})}\right)^{1/2} = \frac{\pi^{1/2}}{2}\mathcal{C}_0,$$

where $\mathcal{C}_0$ was defined in equation (3.8).

We have so far shown the validity of

$$\lim_{t\to\infty}\prod_{p\le t}\frac{\tau_p}{\lambda_p} = \frac{\ell_2 2^{1/2}}{\zeta(n-d)}\left(\lim_{t\to\infty}\prod_{p\le t}\frac{\ell_p}{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}\right)\frac{\pi^{1/2}}{2}\mathcal{C}_0.$$

It is clear that for $p \equiv 1 \pmod 4$ we have $\ell_p = \tau_{f_2}(p)$, and thus (3.53) leads to the absolute convergence of

$$\lim_{t\to\infty}\prod_{\substack{p\equiv 1(\mathrm{mod}\ 4)\\ p\le t}}\ell_p = \prod_{p\equiv 1(\mathrm{mod}\ 4)}\tau_{f_2}(p).$$

By Proposition 3.5.11 one gets

$$\prod_{\substack{p\equiv 3 (\mathrm{mod}\ 4)\\ p\leq t}} \frac{\ell_p}{(1-\frac{1}{p})} = \prod_{\substack{p\equiv 3 (\mathrm{mod}\ 4)\\ p\leq t}} E_\phi(p).$$

It is now clear from Lemma 3.5.9 that the last product converges. Therefore the product $\prod_p \tau_p/\lambda_p$ is convergent, which proves *(2)*.

For the proof of *(3)* we note that the arguments at the end of the proof of *(2)* provided us with the equality

$$\prod_p \frac{\tau_p}{\lambda_p} = \frac{\ell_2 2^{1/2}}{\zeta(n-d)} \left(\prod_{p\equiv 1 (\mathrm{mod}\ 4)} \tau_{f_2}(p) \right) \left(\prod_{p\equiv 3 (\mathrm{mod}\ 4)} E_\phi(p) \right) \frac{\pi^{1/2}}{2} \mathcal{C}_0.$$

We have $E_\phi(2) = \ell_2$ due to Proposition 3.5.18. Recalling Lemma 3.5.9 we get

$$\prod_p \frac{\tau_p}{\lambda_p} = \frac{2^{1/2}}{\zeta(n-d)} \mathbb{L}_\phi \frac{\pi^{1/2}}{2} \mathcal{C}_0.$$

A comparison with (3.40) makes the proof of *(3)* immediately apparent. □

Let us remark that the arguments in the proof of Theorem 3.5.23 can be easily rearranged to show that $\prod_{p\leq t} \tau_p$ diverges. Therefore the numbers λ_p can be viewed as 'convergence factors'. We are very grateful to Daniel Loughran for suggesting this choice for λ_p, as well as for the L-function in (3.65).

In fact, the above proof of *(1)* shows a stronger statement. We thank Jean-Louis Colliot-Thélène for asking the question that prompted us to recognize this.

THEOREM 3.5.25. *If for every prime p there exists a smooth fibre with a $\mathbb{Q}_p$-point, and moreover there exists a smooth fibre with an $\mathbb{R}$-point, then c_ϕ is positive.*

Proof. We have seen in Lemma 3.5.9 that the product

$$\mathbb{L}_\phi = E_\phi(2) \prod_{p\equiv 1 (\mathrm{mod}\ 4)} \tau_{f_2}(p) \prod_{p\equiv 3 (\mathrm{mod}\ 4)} E_\phi(p)$$

converges absolutely. Hence its value is positive if the values of the individual factors are positive. In the proof of Theorem 3.5.23 we showed

that each of the factors in the product above is positive by starting with a $\mathbb{Q}$-point and considering it as a $\mathbb{Q}_p$-point for every p. However, every individual prime was then treated separately, so one may as well have started with $\mathbb{Q}_p$-points for every p which are not necessarily defined over $\mathbb{Q}$.

The same strategy was used to prove $\mathfrak{J} > 0$, and again here one might have started with an $\mathbb{R}$-point that is not necessarily also defined over $\mathbb{Q}$. □

Remark 3.5.26. Theorem 3.5.25 shows that the Hasse principle holds for the total space of smooth fibres. Since the main term in Theorem 3.1.3 only takes care of smooth fibres, the singular fibres lie outside the reach of the proof.