ACTA ARITHMETICA
102.3 (2002)

Sums of two powers of linear forms

by

LEONHARD SUMMERER (Wien)

Introduction. In this paper we are interested in the proportion of forms $F(\mathbf{X}) = F(X_1, \ldots, X_n)$ of degree m with integral coefficients which can be written as $L_1(\mathbf{X})^m + L_2(\mathbf{X})^m$ with arbitrary linear forms L_1, L_2 with algebraic coefficients.

We consider forms

$$F(\mathbf{X}) = \sum_{\alpha} q_\alpha \mathbf{X}^\alpha = \sum_{\alpha_1+\ldots+\alpha_n=m} q_{\alpha_1\ldots\alpha_n} X_1^{\alpha_1} \ldots X_n^{\alpha_n} \tag{1}$$

with coefficients q_α in $\mathbb{Z}$ and define their height $H(F)$ to be the maximum modulus of these coefficients.

Write $Z(n,m,X)$ for the number of such forms F with $H(F) \le X$ which can be written as

$$F(\mathbf{X}) = L_1(\mathbf{X})^m + L_2(\mathbf{X})^m,$$

where L_1, L_2 are linear forms.

Our main result is as follows:

THEOREM 1.1. *For $m \ge 3$ and $n > 4m$,*

$$Z(n,m,X) \asymp X^{2n/m},$$

with the constants implicit in $\asymp$ depending only on n and m.

The particular quantity $Z(n,3,X)$ was estimated by the author in [Su], the result there is covered by Theorem 1.1.

Two challenging open problems should be mentioned in this context (see also [K], [E-K]):

Write $Z_r(n,m,X)$ for the number of forms F as in (1) with $H(F) \le X$ which can be written as

$$F(\mathbf{X}) = L_1(\mathbf{X})^m + \ldots + L_r(\mathbf{X})^m.$$

The estimate of $Z_r(n,m,X)$ for $r > 2$ remains open.

2000 *Mathematics Subject Classification*: 11E76, 11H46, 11H06.

Write $Z(n,f,X)$ for the number of forms F as in (1) with $H(F)\le X$ that have a representation

$$F(\mathbf{X})=f(L_1(\mathbf{X}),L_2(\mathbf{X}))$$

where f is a binary form of degree m over $\mathbb{Z}$ and L_1,L_2 are linear forms. The estimate of $Z(n,f,X)$ represents a generalization of Theorem 1.1 in another sense. Some of our methods, especially in Section 2, readily apply to this more general situation.

1. The outline of the proof. We start with the observation that forms F counted in $Z(n,m,X)$ are the mth power of one single linear form L (which we then call *degenerate*) precisely when the linear forms L_1 and L_2 have proportional coefficient vectors $\mathbf{a}$ and $\mathbf{b}$. Their number is of order of magnitude $X^{n/m}$ for $n\ge m$ and we may exclude this case from our considerations and focus on non-degenerate forms.

The crucial fact and thus the base for all further investigation is contained in

PROPOSITION 1.1. *Let F be a non-degenerate form of degree m over $\mathbb{C}$. If*

$$F(\mathbf{X})=L_1(\mathbf{X})^m+L_2(\mathbf{X})^m=M_1(\mathbf{X})^m+M_2(\mathbf{X})^m,$$

then, after a suitable permutation of M_1,M_2,

$$L_1^m=M_1^m\quad\text{and}\quad L_2^m=M_2^m,$$

so that $L_1=\zeta M_1$ and $L_2=\xi M_2$, with mth roots of unity ζ,ξ.

Proof. Since L_1,L_2 are linearly independent, $\operatorname{grad}F=0$ precisely on the space $L_1=L_2=0$, which is therefore determined by F, and is thus the same as the space $M_1=M_2=0$. Therefore $L_1=\alpha_1M_1+\alpha_2M_2$ and $L_2=\beta_1M_1+\beta_2M_2$ and we obtain a system

$$(\star)\qquad\begin{aligned}&\alpha_1^{m-j}\alpha_2^j+\beta_1^{m-j}\beta_2^j=1=\alpha_1^j\alpha_2^{m-j}+\beta_1^j\beta_2^{m-j}\quad&&\text{for } j\in\{0,m\},\\&\alpha_1^{m-j}\alpha_2^j+\beta_1^{m-j}\beta_2^j=0=\alpha_1^j\alpha_2^{m-j}+\beta_1^j\beta_2^{m-j}\quad&&\forall j:1\le j\le m-1.\end{aligned}$$

If $\alpha_1\alpha_2\ne0$, we must have $\beta_1\beta_2\ne0$ and $(\star)$ for $j=1$ implies

$$(\alpha_1/\beta_1)^{m-1}=-(\beta_2/\alpha_2)\quad\text{and}\quad(\alpha_1/\beta_1)=-(\beta_2/\alpha_2)^{m-1},$$

so that after a little computation

$$(\alpha_1/\beta_1)^{m^2-2m}=(-1)^m.$$

For $j=2$, $(\star)$ implies further

$$(\alpha_1/\beta_1)^{m-2}=-(\beta_2/\alpha_2)^2\quad\text{and}\quad(\alpha_1/\beta_1)^2=-(\beta_2/\alpha_2)^{m-2},$$

and a similar computation shows

$$(\alpha_1/\beta_1)^{m^2-4m}=(-1)^m.$$

The combination of these two facts yields $(\alpha_1/\beta_1)^{2m} = 1$ and we obtain

$$\alpha_1^m = \beta_1^m, \quad \alpha_2^m = \beta_2^m \quad \text{or} \quad \alpha_1^m = -\beta_1^m, \quad \alpha_2^m = -\beta_2^m.$$

Comparing coefficients in the case $j = 0$, we see that the right hand equalities cannot be satisfied, whereas for $j = 1, 2$ the left hand equalities would give

$$\beta_1\alpha_2 + \alpha_1\beta_2 = 0 = \beta_1^2\alpha_2^2 + \alpha_1^2\beta_2^2,$$

which contradicts the assumption $\alpha_i\beta_j \neq 0$. If $\alpha_2 = 0$, then $\beta_2 \neq 0, \beta_1 = 0$, and we get $\alpha_1^m = \beta_2^m$, hence the desired conclusion follows. If $\alpha_1 = 0$, we get $\beta_1 \neq 0, \beta_2 = 0$ and we have to interchange M_1, M_2 to fall under the case $\alpha_2 = 0$ again.

The uniqueness of the representation of non-degenerate forms of degree m implies the existence of representations over certain number fields for rational forms. Let $F(\mathbf{X}) = (\sum a_iX_i)^m + (\sum a_i'X_i)^m$ and K be the field generated by the quotients a_i/a_j $(1 \leq i, j \leq n; a_j \neq 0)$.

Corollary 1.2. *The field K depends only on the form F. It is either the rational field or a quadratic number field. When K is rational, also the quotients a_i'/a_j' are rational; when K is quadratic, then a_i'/a_j' $(1 \leq i, j \leq n; a_j' \neq 0)$ is the conjugate of a_i/a_j in K. There exist representations $F(\mathbf{X}) = \lambda(\sum a_iX_i)^m + \lambda'(\sum a_i'X_i)^m$ where $a_1, \ldots, a_n, a_1', \ldots, a_n', \lambda, \lambda'$ are in K, and if K is quadratic, the pairs λ, λ' respectively a_i, a_i' $(i = 1, \ldots, n)$ are pairs of conjugates.*

Proof. By Proposition 1.1 the pair of points $(a_1 : \ldots : a_n), (a_1' : \ldots : a_n')$ in $(n-1)$-dimensional projective space is uniquely determined by the form F. Every automorphism either leaves these two points fixed (i.e., leaves the quotients a_i/a_j and a_i'/a_j', when defined, fixed), or interchanges these two points (i.e., interchanges a_i/a_j and a_i'/a_j'). If every automorphism is of the first kind, then $K = \mathbb{Q}$ and all the quotients a_i/a_j and a_i'/a_j' lie in $\mathbb{Q}$. If there is an automorphism of the second kind, then K is quadratic and a_i/a_j and a_i'/a_j' are conjugates in K.

There are representations of F with $(a_1, \ldots, a_n)$ and $(a_1', \ldots, a_n')$ in K^n and these vectors are not proportional. Hence if $K = \mathbb{Q}$, every automorphism maps $\lambda(\sum a_iX_i)^m, \lambda'(\sum a_i'X_i)^m$ into themselves, and therefore $\lambda, \lambda' \in \mathbb{Q}$. If K is quadratic, an automorphism may also interchange the two summands of F. Since the coefficients of the two appearing linear forms are respective conjugates in K, the same must hold for λ, λ'.

Definition 1.3. We call a non-degenerate form of degree m over $\mathbb{Q}$ which has a representation of the shape

$$F(\mathbf{X}) = \lambda\Big(\sum a_iX_i\Big)^m + \lambda'\Big(\sum a_i'X_i\Big)^m$$

with $\lambda, \lambda', a_i, a_i' \in \mathbb{Q}$, $i = 1, \ldots, n$, *representable over* $\mathbb{Q}$.

Otherwise by Corollary 1.2 there exists a uniquely determined quadratic number field $\mathbb{Q}(\sqrt{d})$ in which $\lambda, \lambda', a_i, a_i'$ $(i = 1, \ldots, n)$ lie and are conjugates respectively. We then call $\mathbb{Q}(\sqrt{d})$ the *representation field of* F.

As a consequence of these results, we first split $Z(n,m,X)$ into the quantities $Z(d,n,m,X)$, which refer to the possible representation fields of the forms in question. With these notations, the uniqueness of the number field associated to each form yields

$$Z(n,m,X) = \sum_{\substack{d\neq 0\\ \text{sq-free}}} Z(d,n,m,X),$$

and with a view toward the estimate of $Z(n,m,X)$ we may first count all forms with representation field $\mathbb{Q}(\sqrt{d})$ for fixed d, and then sum over all these number fields.

Theorem 1.4. *Let $n > 2m$ and $h = h(d)$ be the class number of the quadratic number field $\mathbb{Q}(\sqrt{d})$. Then there exists a constant $C > 0$, depending on m only, with*

$$Z(d,n,m,X) \ll X^{2n/m} h^2(d) C^{\omega(d)} |d|^{-n/(2m)},$$

where $\omega(d)$ denotes the number of distinct prime factors of d, and the implied constant in $\ll$ depends only on n and m.

The proof of this theorem will only be given at the end of the paper, but meanwhile we will show how Theorem 1.1 can be deduced from the above result if we use a well known estimate for the class number of quadratic number fields:

Proposition 1.5. *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic number field with class number $h(d)$. Then for all $\varepsilon > 0$,*

$$h(d) \ll |d|^{1/2+\varepsilon}.$$

Moreover, if $d < 0$, then $h(d) \sim |d|^{1/2}$, and the exponent $1/2$ cannot be improved.

Proof. This is an immediate consequence of Dirichlet's class number formula (see e.g. [NRRL, p. 91, Theorem 8]).

Deduction (of Theorem 1.1): Theorem 1.4 yields, for $n > 2m$,

$$\begin{aligned} Z(n,m,X) &= \sum_{\substack{d\neq 0\\ \text{sq-free}}} Z(d,n,m,X) \ll \sum_{\substack{d\neq 0\\ \text{sq-free}}} X^{2n/m} h^2(d) C^{\omega(d)} |d|^{-n/(2m)} \\ &= X^{2n/m} \sum_{\substack{d\neq 0\\ \text{sq-free}}} h^2(d) C^{\omega(d)} |d|^{-n/(2m)}. \end{aligned}$$

Proposition 1.5 then gives $h(d) \ll |d|^{1/2+\varepsilon}$ for $\varepsilon > 0$ and it is clear that $C^{\omega(d)} \ll |d|^{\varepsilon}$ for $\varepsilon > 0$ with the implied constant depending on m, ε only. Neglecting the condition that d be square-free we find

$$Z(n,m,X) \ll X^{2n/m} \sum_{d=1}^{\infty} d^{1-n/(2m)+\varepsilon}.$$

Now $1 - n/(2m) + \varepsilon < -1 - 1/(2m) + \varepsilon < -1$ for $n > 4m$ and ε small, so that our sum is convergent, and we finally obtain

$$Z(n,m,X) \ll X^{2n/m}.$$

To round up our discussion of $Z(n,m,X)$, it remains to give a lower bound for this quantity. This turns out to be trivial since every pair of non-collinear vectors $((a_1,\ldots,a_n),(b_1,\ldots,b_n)) \in \mathbb{Z}^n \times \mathbb{Z}^n$ with $|a_i|, |b_i| \le c(n)X^{1/m}$ determines a form of the required shape via

$$F(\mathbf{X}) = \Big(\sum a_i X_i\Big)^m + \Big(\sum b_i X_i\Big)^m.$$

The estimate

$$Z(n,m,X) \gg X^{2n/m}$$

follows immediately.

Within a given number field, the representation of a given form F as

$$F(\mathbf{X}) = \lambda\Big(\sum a_i X_i\Big)^m + \lambda'\Big(\sum a_i' X_i\Big)^m$$

with $\lambda, \lambda', a_i, a_i' \in \mathbb{Q}(\sqrt{d})$ for $i = 1,\ldots,n$, which are supposed to be conjugates for $d \ne 1$, is far from being unique (e.g., a_i, a_i' may be replaced by $\nu a_i, \nu a_i'$).

Our next task is therefore to reduce the number of possible representations belonging to the same F, in order to be able to sum over all representations to consider. This amounts to imposing conditions on the pair (λ, λ') that appears in some representation of F.

Definition 1.6. Let F be a form of degree m counted by $Z(d,n,m,X)$ in the representation of Definition 1.3. Then we call (λ, λ') the *leading coefficient pair* of F in this representation, and we identify (λ, λ') with (λ', λ). In the case $d = 1$ we get in this way a pair of rational numbers and for $d \ne 1$ a pair of conjugate numbers from the given quadratic number field.

As already noticed, the leading coefficient pair is not uniquely determined for a given form, but it is an easy matter to show that there is always a representation of F with integer leading coefficient pair and that moreover two such pairs differ only by an mth power in the respective representation field in each component.

This leads us straight to the question of finding a sufficiently small set that contains a system of representatives for $\mathbb{Q}(\sqrt{d})^*/(\mathbb{Q}(\sqrt{d})^*)^m$. This makes it necessary to pass to ideals, since $\mathcal{O}_d$ need not be a factorial ring.

Let $h = h(d)$ be the class number of $\mathbb{Q}(\sqrt{d})$ and $\mathcal{A}_1, \ldots, \mathcal{A}_h$ the distinct ideal classes, where it is assumed that $\mathcal{A}_1$ is the principal class. We then choose from each class an integer prime ideal $\wp_i \in \mathcal{A}_i$ that is relatively prime to $2md$ such that when $\mathcal{A}_i \neq \mathcal{A}_1$ and $\mathcal{A}_j = \mathcal{A}_i^{-1}$, then $\wp_j = \wp_i'$. This choice is possible, for in each class one can find a prime ideal that is relatively prime to a given one (see e.g. [N, p. 22, exercise 5]). Once such a $\wp_i$ is chosen for $\mathcal{A}_i, i \neq 1$, the conjugate $\wp_i'$ obviously lies in $\mathcal{A}_i^{-1}$ and satisfies all requirements as well.

A series of standard arguments from algebraic number theory allow us to prove:

PROPOSITION 1.7. *Let π_{ia} be elements in $\mathcal{O}_d$ satisfying $(\pi_{ia}) = \wp_i^m a, 1 \leq i \leq h$, with integral and mth power free $a \in \langle \wp_i^m \rangle^{-1}$ and let ε_j, $1 \leq j \leq w$ be units in U_d that build up a system of representatives of U_d/U_d^m. Then the set $\{\varepsilon_j \pi_{ia} \mid 1 \leq j \leq w, 1 \leq i \leq h,\ a \text{ as above}\}$ contains a system of representatives Π for $\mathbb{Q}(\sqrt{d})^*/(\mathbb{Q}(\sqrt{d})^*)^m$.*

Proof. We have to show that any $\lambda \in \mathbb{Q}(\sqrt{d})$ may be written as $\lambda = \varepsilon_j \pi_{ia} b^m$ with ε_j, π_{ia} as indicated for suitable b in $\mathbb{Q}(\sqrt{d})$. Let therefore (λ) be the principal ideal generated by λ. Then we may write $(\lambda) = a_0^m a$ uniquely with an mth power free integral ideal a. Choosing the representative $\wp_i$ of the ideal class $\mathcal{A}_i$ in which a_0 lies, we have

$$(\lambda) = \wp_i^m a \wp_i^{-m} a_0^m = \wp_i^m a (\wp_i^{-1} a_0)^m,$$

where $\wp_i^{-1} a_0$ is principal by construction, and thus the same is true for $\wp_i^m a$, which shows that $a \in \langle \wp_i^m \rangle^{-1}$. We have thus found some $i \in \{1, \ldots, h\}$ and an integral ideal $a \in \langle \wp_i^m \rangle^{-1}$ such that $(\lambda) = \wp_i^m a$ modulo mth powers of principal ideals. If we let $\pi_{ia} \in \mathcal{O}_d$ be such that $(\pi_{ia}) = \wp_i^m a$, the element π_{ia} is determined up to a unit $\varepsilon \in U_d$ and for the required representation $\lambda = \varepsilon \pi_{ia} b^m$ we may obviously choose ε in a set of representatives of U_d/U_d^m. This set is trivially finite for $d < 0$ and by Dirichlet's Unit Theorem for $d > 0$ as well, which concludes the proof.

A bound for $Z(d, n, m, X)$ is thus obtained by counting all representations of forms in question whose leading coefficient pair lies in the subset of $\Pi \times \Pi$ for which (λ, λ') is a pair of conjugates for $d \neq 1$. We denote this set by Π_d and by $Z((\lambda, \lambda'), d, n, m, X)$ the number of forms counted in $Z(d, n, m, X)$ which have leading coefficient pair (λ, λ'). We may thus resume the preceding observations in the form

$$Z(d, n, m, X) = \sum_{(\lambda, \lambda') \in \Pi_d} Z((\lambda, \lambda'), d, n, m, X),$$

which turns out to be the crucial quantity to estimate. Special attention has to be paid to the dependence of all the constants on (λ, λ') and on d, in view of a later summation over these parameters.

2. Some basic inequalities. Throughout this section, we recall the fact already mentioned in the introduction, that

$$Z(n, m, X) = Z(n, f, X) \quad \text{with} \quad f(X, Y) = X^m + Y^m,$$

and since the following observations readily apply to arbitrary forms f of degree m, we may as well treat the general case, keeping in mind $f(X, Y) = X^m + Y^m$ as an example. We thus have to consider forms F that have a representation

$$F(\mathbf{X}) = f\Big(\sum a_i X_i, \sum b_i X_i\Big)$$

with algebraic coefficients $(a_i, b_i)_{i=1,\ldots,n}$.

In order to study n-tuples (a_i, b_i) that guarantee that F is counted in $Z(n, f, X)$, we have to bring into evidence the assumptions

$$|q_\alpha|_p \le 1 \quad \forall p \in \mathbb{P} \quad \text{and} \quad |q_\alpha|_\infty \le X$$

for the coefficients of F.

For this purpose, we use the fact that $\mathbb{Z}[X, Y]$ is a unique factorization domain to write

$$f(X, Y) = l_1(X, Y) \ldots l_m(X, Y),$$

where $l_1, \ldots, l_m$ are linear forms with coefficients in a splitting field $\mathbb{Q}(f)$ of f and these m factors are uniquely determined up to a constant factor. Applying this decomposition to F we find

$$F(\mathbf{X}) = l_1\Big(\sum a_i X_i, \sum b_i X_i\Big) \ldots l_m\Big(\sum a_i X_i, \sum b_i X_i\Big),$$

and this quantity has to be an integer for any $\mathbf{X} \in \mathbb{Z}^n$. In particular, we may choose $X_i = 1$ and $X_j = 0$ for $i \ne j$ to obtain the coefficient $q_{0,\ldots,m,\ldots,0}$ of F, which implies

$$|l_1(a_i, b_i) \ldots l_m(a_i, b_i)|_p \le 1 \quad \forall p,$$
$$|l_1(a_i, b_i) \ldots l_m(a_i, b_i)|_\infty \le X.$$

If we abbreviate $l_j(a_i, b_i)$ by l_j^i and consider products of the linear forms $l_1, \ldots, l_m$ involving different variables, i.e. expressions of the type $l_1^{i_1} \ldots l_m^{i_m}$ with $i_j \in \{1, \ldots, n\}$ for $1 \le j \le m$, we cannot expect the same result since this mixed product will in general not be a rational number.

Nevertheless a similar result holds for valuations in the field K obtained by adjoining to $\mathbb{Q}(f)$ all the $a_i, b_i, 1 \le i \le n$:

Proposition 2.1. *There is a positive constant $c(n,m)$ such that for every $(i_1,\dots,i_m)\in\{1,\dots,n\}^m$, we have*

$$|l_1^{i_1}\dots l_m^{i_m}|_v\le 1 \quad \textit{for } v\in M_0(K), \textit{ the non-archimedean valuations of } K,$$
$$|l_1^{i_1}\dots l_m^{i_m}|_v\le c(n,m)X \quad \textit{for } v\,|\,\infty, \textit{ the archimedean valuations of } K.$$

Proof. If $F=F_1\dots F_d$ is some decomposition of F with polynomials $F_i=F_i(\mathbf{X})$ in n variables, [La, Proposition 2.1, Sec. 3] asserts that $|F_1|_v\dots|F_d|_v=|F|_v$ for all non-archimedean valuations v. Proposition 2.3 in the same text handles the case of archimedean valuations as well: if $\deg f\le m$, then $|F_1|_v\dots|F_d|_v\le c(n,m)|F|_v$ for $v\,|\,\infty$ with some positive constant depending on n,m only.

In the present context, let $F(\mathbf{X})=L_1(\mathbf{X})\dots L_m(\mathbf{X})$, where $L_j(\mathbf{X})=l_j(\sum a_iX_i,\sum b_iX_i)$, hence

$$(\max_{i_1}|l_1^{i_1}|_v)\dots(\max_{i_m}|l_m^{i_m}|_v)\le c(n,m)X$$

as claimed.

After this treatment of forms F represented by arbitrary binary forms f, it is time to come back to the case $f(X,Y)=X^m+Y^m$ or even better $f(X,Y)=\lambda X^m+\lambda' Y^m$. Instead of the variables (a_i,b_i) we have $(a_i,a_i')\in\mathbb{Q}(\sqrt{d})^2$ where a_i and a_i' are conjugates for $d\neq 1$ and independent rationals for $d=1$. For the following it will even be convenient to deal with rational variables only; we obtain this by the change of variables

$$a_i=A_i+B_i\sqrt{d} \quad\text{and}\quad a_i'=A_i-B_i\sqrt{d}$$

with $(A_i,B_i)\in\mathbb{Q}^2$. The factors in the decomposition of $f(a_i,a_i')$ thus become

$$\begin{aligned}l_j(a_i,a_i')&=\lambda^{1/m}a_i+\lambda'^{1/m}\zeta^{2j-1}a_i'\\&=(\lambda^{1/m}-\zeta^{2j-1}\lambda'^{1/m})A_i+(\lambda^{1/m}+\zeta^{2j-1}\lambda'^{1/m})\sqrt{d}\,B_i,\end{aligned}$$

where ζ is a primitive $2m$th root of unity, and we have

$$K=\mathbb{Q}(\sqrt{d},\zeta,\lambda^{1/m},\lambda'^{1/m})$$

so that $[K:\mathbb{Q}]\le 4m^3$. By abuse of notation, we write $l_j(A_i,B_i)$ for this expression, and $(\mathbf{A},\mathbf{B})$ for the n-tuple $(A_i,B_i)_{i=1,\dots,n}$.

3. The archimedean bound. In this section we study rational solutions $(A_i,B_i)_{i=1,\dots,n}$ of the inequalities

$$|l_1^{i_1}\dots l_m^{i_m}|_v\le c(n,m)X \quad\text{for } v\,|\,\infty,$$

obtained in the last section. We abbreviate $c:=c(n,m)$ and consider the following domains $S_0(X)$ and $S(X)$:

Definition 3.1. Let $S_0(X) \subset \mathbb{R}^2$ be the domain defined by

$$S_0(X) := \{(A,B) \in \mathbb{R}^2 : |l_1(A,B)\dots l_m(A,B)|_\infty \le X\}.$$

By $S(X)$ we denote the domain in $\mathbb{R}^{2n}$ defined by

$$S(X) := \{(\mathbf{A},\mathbf{B}) \in \mathbb{R}^{2n} : |l_1^{i_1}\dots l_m^{i_m}|_v \le cX \text{ for } v \mid \infty \text{ and any } (i_1,\dots,i_m)\}.$$

Proposition 3.2. *Let $f = l_1\dots l_m$ be the decomposition of the binary form $f(X,Y) = \lambda X^m + \lambda' Y^m$. For $1 \le s \le m$, $k = 0,1,2,\dots$, let $P_s^{(k)}$ be the set in $\mathbb{R}^2$ defined by the inequalities*

$$|l_s|_v \le 2^{-(m-1)k}(cX)^{1/m},$$
$$\Big|\prod_{j\ne s} l_j\Big|_v \le 2^{(m-1)(k+1)}(cX)^{(m-1)/m}.$$

Then if $(\mathbf{A},\mathbf{B})$ lies in $S(X)$, there exist s,k such that each component (A_i,B_i) of $(\mathbf{A},\mathbf{B})$ lies in $P_s^{(k)}$.

Proof. For $1 \le j \le m$, pick i_j with $|l_j^{i_j}|_v = \max_i |l_j^i|_v$, where as above $l_j^i = l_j(A_i,B_i)$. By Proposition 2.1,

$$|l_1^{i_1}\dots l_m^{i_m}|_v \le cX.$$

Pick s with $|l_s^{i_s}|_v = \min_j |l_j^{i_j}|_v$, and then pick $k \in \mathbb{Z}$ with

$$2^{-(m-1)(k+1)}(cX)^{1/m} < |l_s^{i_s}|_v < 2^{-(m-1)k}(cX)^{1/m}.$$

In view of the aforementioned result of Proposition 2.1 and the minimality of $|l_s^{i_s}|_v$, we have $k \ge 0$ and we obtain

$$\Big|\prod_{j\ne s} l_j\Big|_v < 2^{(m-1)(k+1)}(cX)^{-1/m}(cX) = 2^{(m-1)(k+1)}(cX)^{(m-1)/m}.$$

By the choice of i_j maximizing $|l_j^{i_j}|_v$, for each i, $1 \le i \le n$, we have

$$|l_s^i|_v \le 2^{-(m-1)k}(cX)^{1/m} \quad \text{and} \quad \Big|\prod_{j\ne s} l_j^i\Big|_v \le 2^{(m-1)(k+1)}(cX)^{(m-1)/m};$$

thus indeed each $(A_i,B_i) \in P_s^{(k)}$.

As a consequence of this result we have

$$S(X) \subset \bigcup_{k=1}^{\infty}\bigcup_{s=1}^{m} (P_s^{(k)})^n,$$

so that we may focus only on the two-dimensional pieces $P_s^{(k)}$ that build up $S_0(X)$. However, it will be convenient to deal with convex sets containing these $P_s^{(k)}$ and whose volumes may be bounded explicitly in $k, (\lambda,\lambda')$ and d.

Lemma 3.3. *For $k \geq 0$ we have*

$$V(P_s^{(k)}) \ll 2^{-k} d^{-1/2} (\lambda\lambda')^{-1/m} X^{2/m},$$

where the constant in $\ll$ depends on n and m only.

Proof. Notice that the inequality

$$\Big| \prod_{j \neq s} l_j \Big|_v \leq 2^{(m-1)(k+1)} (cX)^{(m-1)/m}$$

implies the existence of some $r \neq s$ with $|l_r|_v \leq 2^{k+1}(cX)^{1/m}$ since not all the $m-1$ factors can be greater than their geometric mean and we have to deal with the system

$$|l_s|_v \leq 2^{-(m-1)k}(cX)^{1/m}, \quad |l_r|_v \leq 2^{k+1}(cX)^{1/m}.$$

We start with the observation that the volume of the domain given by the inequalities

$$|tA + uB| \leq X \quad \text{and} \quad |vA + wB| \leq Y$$

is $XY/|tw - uv|$. In the application below the coefficients t, u, v, w are the ones of the linear forms l_s and l_r (see Section 2); in particular

$$|tw - uv| = (\lambda\lambda')^{1/m}(\zeta^{2r-1} - \zeta^{2s-1}),$$

so that $|tw - uv| \gg |\lambda\lambda'|^{1/m}$. Moreover $XY = 2^{-(m-2)k+1}(cX)^{2/m}$ and we indeed obtain

$$V(P_s^{(k)}) \ll 2^{-k} d^{-1/2} (\lambda\lambda')^{-1/m} X^{2/m},$$

since the change of variables from $(a_i, a_i') \in \mathbb{Q}(\sqrt{d})$ to rational (A_i, B_i) from Section 2 has determinant $1/2\sqrt{d}$.

From now on we will refer to $P_s^{(k)}$ as the sets defined by the inequalities

$$|l_s|_v \leq 2^{-(m-1)k}(cX)^{1/m}, \quad |l_r|_v \leq 2^{k+1}(cX)^{1/m} \quad \text{for some } r \neq s,$$

which have the same properties as the initial covering sets and the advantage to be convex and symmetric with respect to the origin.

4. The non-archimedean bound. We start by analyzing the inequalities $|l_1^{i_1} \ldots l_m^{i_m}|_v \leq 1$ for $v \mid p$ with a fixed prime p that stem from Proposition 2.1. Our goal is to show that p-adic solutions $(\mathbf{A}, \mathbf{B})$ of these inequalities lie in a finite number of discrete $\mathbb{Z}_p$-modules of $\mathbb{Q}_p^{2n}$, each of which being the n-fold cartesian product of a two-dimensional such module. For this purpose, the main tool is a result about the index of some discrete $\mathbb{Z}_p$-modules determined by a system of equations over an algebraic number field. This result, stated below as Theorem 4.1, was proved by the author in [Su] with the purpose of applying it to the kind of problem in question.

Remark. If A, B are rank r submodules of a free $\mathbb{Z}_p$-module N of rank r, we define the index of B in A by $[A : B] := [M : B]/[M : A]$, where M is a module in N containing both A and B. This index is well defined, since it is independent of the choice of M under the given restrictions.

Theorem 4.1. *Let $p \in \mathbb{P}$ and K be an algebraic number field. For each $v \mid p$ let $\mathcal{A}_v$ be a non-singular $m \times m$ matrix with entries from K_v. Then every $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Q}_p^m$ satisfying $|\mathcal{A}_v \mathbf{x}|_v \le 1$ for $v \mid p$ lies in a discrete $\mathbb{Z}_p$-module $\Lambda_0(p)$ of $\mathbb{Q}_p^m$ of rank m. Moreover*

$$\underline{\Lambda}_0(p) \subset \Lambda_0(p) \subset \overline{\Lambda}_0(p),$$

where $\underline{\Lambda}_0(p)$ denotes the module defined by $|\mathbf{x}|_v \le |\mathcal{A}_v|_v^{-1}$ for all $v \mid p$ and $\overline{\Lambda}_0(p)$ is defined by $|\mathbf{x}|_v \le |\mathcal{A}_v|_v^{m-1} |\det \mathcal{A}_v|_v^{-1}$ for all $v \mid p$. For the index of $\Lambda_0(p)$ in $\mathbb{Z}_p^m$ we have

$$[\mathbb{Z}_p^m : \Lambda_0(p)] \ge \{\max_{v \mid p} |\det \mathcal{A}_v|_v\}_p,$$

where $\{A\}_p := \min\{p^g : g \in \mathbb{Z},\ p^g \ge A\}$ and $|\mathcal{A}_v|_v$ denotes the maximum norm of the entries of $\mathcal{A}_v$.

In order to apply this result, we first restrict ourselves to one pair of variables $(A, B) \in \mathbb{Q}_p^2$ and write l_j for $l_j(A, B)$. This way of proceeding is motivated by the following observation: Since $|l_1^{i_1} \ldots l_m^{i_m}|_v \le 1$ for any choice of $(i_1, \ldots, i_m)$ by Proposition 2.1, this holds in particular for the maximum of all such products. Consequently,

$$\max_i |l_j^i|_v \le p^{z_j^{(v)}} \qquad \text{for } 1 \le j \le m$$

with $z_1^{(v)} + \ldots + z_m^{(v)} \le 0$ and the above system holds for any pair of variables (A_i, B_i) with the same m-tuple $(z_1^{(v)}, \ldots, z_m^{(v)})$. The linear forms l_j having rational variables (A, B) and coefficients from a field K with $[K : \mathbb{Q}] \le 4m^3$, the value group of v is a subset of $(4m^3)^{-1}\mathbb{Z}$ and we may restrict ourselves to m-tuples in this discrete group. For any such m-tuple, we want to single out the two most restrictive ones that define the system

$$(\star) \qquad |l_{j_0}|_v \le p^{z_{j_0}^{(v)}}, \qquad |l_{j_1}|_v \le p^{z_{j_1}^{(v)}},$$

where $j_0 \ne j_1$ and $z^{(v)} := -(z_{j_0} + z_{j_1})$ is maximal.

We have thus shown that each pair of variables (A_i, B_i) of $(\mathbf{A}, \mathbf{B})$ with $|l_1^{i_1} \ldots l_m^{i_m}|_v \le 1$ satisfies $(\star)$ for one of the $m(m-1)$ possible choices of (j_0, j_1), where for given $(\mathbf{A}, \mathbf{B})$ the pair (j_0, j_1) is the same for all two-dimensional components.

This argument applies to any $v \mid p$ and we pick v_0 such that

$$z^{(p)}(\mathbf{A}, \mathbf{B}) := z^{(v_0)}(\mathbf{A}, \mathbf{B}) := \max_{v \mid p} z^{(v)}(\mathbf{A}, \mathbf{B}),$$

and let (l_{j_0}, l_{j_1}) be the pair of linear forms corresponding to the choice of (j_0, j_1) for v_0.

Definition 4.2. To each $(\mathbf{A},\mathbf{B}) \in \mathbb{Q}_p^{2n}$ with $|l_1^{i_1} \ldots l_m^{i_m}|_v \le 1$ for all $v \mid p$, we associate the quantity $z^{(p)}(\mathbf{A},\mathbf{B}) \in (4m^3)^{-1}\mathbb{N}_0$ defined by

$$z^{(p)}(\mathbf{A},\mathbf{B}) := \max_{v|p}\{-\min_{j_0\neq j_1}(z_{j_0}+z_{j_1})\}.$$

Now, what can be said about $|l_{j_0}|_v$ and $|l_{j_1}|_v$ for $v \neq v_0$? From $z_1^{(v)} + \ldots + z_m^{(v)} \le 0$ and $z_1^{(v)} \le \ldots \le z_m^{(v)}$, we obtain $z_m^{(v)} \le \frac{m-1}{2} z^{(p)}$ and thus

$$\begin{aligned} |l_{j_0}|_{v_0} &\le p^{z_{j_0}^{(v_0)}} &\quad\text{and}\quad |l_{j_0}|_v &\le p^{\frac{m-1}{2}z^{(p)}},\\ |l_{j_1}|_{v_0} &\le p^{z_{j_1}^{(v_0)}} &\quad\text{and}\quad |l_{j_1}|_v &\le p^{\frac{m-1}{2}z^{(p)}} \end{aligned}$$

for $v = v_0$ respectively $v \neq v_0$.

Conversely, if $(\mathbf{A},\mathbf{B})$ is given with $z^{(p)}(\mathbf{A},\mathbf{B}) = z^{(p)}$, there are at most $4m^3$ possible choices for the valuation v_0 with $z^{(v_0)} = z^{(p)}$, and once v_0 is fixed, $m(m-1)$ possibilities for the pair of linear forms (l_{j_0}, l_{j_1}).

In order to complete the data in the above system, it remains to estimate the number of $(z_{j_0}^{(v_0)}, z_{j_1}^{(v_0)})$ for which $z^{(p)} = -(z_{j_0}^{(v_0)} + z_{j_1}^{(v_0)})$ in $(4m^3)^{-1}\mathbb{Z}$. By definition of $z^{(p)}$, for $v = v_0$,

$$\begin{aligned} z_{j_1}^{(v)} + \ldots + z_m^{(v)} \le z_{j_0}^{(v)} &\;\Rightarrow\; (m-1)z_{j_1}^{(v)} \le z_{j_0}^{(v)}\\ &\;\Rightarrow\; -(m-1)z^{(p)} \le (m-2)z_{j_0}^{(v)} \;\Rightarrow\; -\frac{m-1}{m-2}z^{(p)} \le z_{j_0}^{(v)}, \end{aligned}$$

which yields $-\frac{m-1}{m-2}z^{(p)} \le z_{j_0}^{(v)} \le 0$ and this leaves only $O_m(z^{(p)})$ possibilities for $z_{j_0}^{(v_0)}$ in $(4m^3)^{-1}\mathbb{Z}$; $z_{j_1}^{(v_0)}$ is then uniquely determined by $z^{(p)} = -(z_{j_0}^{(v_0)} + z_{j_1}^{(v_0)})$.

In order to apply Theorem 4.1 to the given situation (with $m = 2$ variables), we need to bring the system $(\star)$ into a slightly different form. For any linear forms $l_j \neq l_k \in \{l_1, \ldots, l_m\}$ we denote by $L_{j,k}$ the matrix consisting of the coefficients of l_j and l_k and by $\varDelta_{j,k}$ its determinant. In this case

$$\begin{pmatrix} \lambda^{1/m} & -\zeta^{2j-1}\lambda'^{1/m} \\ \lambda^{1/m} & -\zeta^{2k-1}\lambda'^{1/m} \end{pmatrix}\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}$$

yields $\varDelta_{j,k} = (\zeta^{2j-1} - \zeta^{2k-1})(\lambda\lambda')^{1/m}(-2\sqrt{d})$. Notice that only the first factor depends on (j,k) and that

$$\begin{aligned} |\varDelta_{j,k}|_v &= |\zeta^{2j-1} - \zeta^{2k-1}|_v |2^{2m}(\lambda\lambda')^2 d^m|_v^{1/(2m)}\\ &=: |\zeta^{2j-1} - \zeta^{2k-1}|_v |\varDelta|_v^{1/(2m)}, \end{aligned}$$

where $\varDelta \in \mathbb{Z}$ and thus $|\varDelta|_v = |\varDelta|_p$ for $v \,|\, p$. In view of the identity

$$2m = (1-\zeta)\ldots(1-\zeta^{2(k-j)})\ldots(1-\zeta^{2m-1})$$

it is an easy exercise to show that $|\zeta^{2j-1} - \zeta^{2k-1}|_v \geq |2m|_v = |2m|_p$ and we obtain

$$|\varDelta_{j,k}|_v \geq |2m|_p |\varDelta|_p^{1/(2m)},$$

which is independent of $v \,|\, p$.

Now we are in a position to apply Theorem 4.1 with

$$\mathcal{A}_{v_0} := \begin{pmatrix} p^{z_{j_0}^{(v_0)}} & 0 \\ 0 & p^{z_{j_1}^{(v_0)}} \end{pmatrix} L_{j_0,j_1},$$

$$\mathcal{A}_v := \begin{pmatrix} p^{\frac{m-1}{2} z^{(p)}} & 0 \\ 0 & p^{\frac{m-1}{2} z^{(p)}} \end{pmatrix} L_{j_0,j_1} \quad \text{for } v \,|\, p,\ v \neq v_0.$$

Corollary 4.3. *For given $z^{(p)}$, there is a positive constant $c_1(m)$, depending on m only, such that the n-tuples $(A_i, B_i)_{i=1,\ldots,n}$ of rational numbers satisfying $\mathbf{z}(\mathbf{A},\mathbf{B}) = z^{(p)}$ lie in the union of $c_1(m)$ discrete $\mathbb{Z}_p$-modules $\varLambda(p)$ of $\mathbb{Q}_p^{2n}$ for which $\varLambda(p) = \varLambda_0(p)^n$, where $\varLambda_0(p)$ is a discrete $\mathbb{Z}_p$-module in $\mathbb{Q}_p^2$ with*

$$\det \varLambda_0(p) := [\mathbb{Z}^2 : \varLambda_0(p)] \geq \{|2m|_p |\varDelta|_p^{1/(2m)} p^{z^{(p)}}\}_p.$$

Proof. By assumption $z^{(p)}(\mathbf{A},\mathbf{B}) = z^{(p)}$ and the aforementioned arguments yield that each component $\mathbf{X} = (A_i, B_i)$ of $(\mathbf{A},\mathbf{B})$ satisfies $|\mathcal{A}_v \mathbf{X}|_v \leq 1$ for $v \,|\, p$ for some pair $(z_{j_0}^{(v_0)}, z_{j_1}^{(v_0)})$ defined above, the number of resulting systems of matrices $(\mathcal{A}_v, v \,|\, p)$ is bounded by $c_1(m) z^{(p)}$ and each of the $\mathcal{A}_v$ is non-singular, as required. Moreover

$$\max_{v|p} |\det \mathcal{A}_v|_v = |\det \mathcal{A}_{v_0}|_{v_0} \geq p^{z^{(p)}} |2m|_p |\varDelta|_p^{1/(2m)},$$

and each two-dimensional component (A_i, B_i) of $(\mathbf{A},\mathbf{B})$ lies in a discrete $\mathbb{Z}_p$-module $\varLambda_0(p)$ of index

$$[\mathbb{Z}^2 : \varLambda_0(p)] \geq \{|2m|_p |\varDelta|_p^{1/(2m)} p^{z^{(p)}}\}_p.$$

Since the choice of (j_0, j_1) that determines $z^{(p)}$ is independent of the pair of variables (A_i, B_i), we obtain $\varLambda(p) = \varLambda_0(p)^n$ as desired.

Our next task is to combine the results of Corollary 4.3 for all $p \in \mathbb{P}$. For this purpose, we again refer to a general result of the author that establishes the connection between the discrete $\mathbb{Z}_p$-modules of Theorem 4.1 and the lattice built up by the rational points that lie in all those p-adic lattices. We state this result here without proof, the details may be found in [Su].

Theorem 4.4. *Let K be an algebraic number field and suppose that for every valuation $v \in M_0(K)$ we are given a non-singular $m \times m$ matrix $\mathcal{A}_v$ with entries from K, such that $\mathcal{A}_v \equiv I_m \bmod v$ for almost all $v \in M_0(K)$. For $p \in \mathbb{P}$ let $\Lambda_0(p)$ be the discrete $\mathbb{Z}_p$-module of $\mathbb{Q}_p^m$ of Theorem 4.1 consisting of $\mathbf{y} = (y_1, \ldots, y_m) \in \mathbb{Q}_p^m$ that satisfy $|\mathcal{A}_v \mathbf{y}|_v \leq 1$ for all $v \,|\, p$. Then every $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Q}_p^m$ satisfying $|\mathcal{A}_v \mathbf{x}|_v \leq 1$ for all $v \in M_0(K)$ lies in the lattice Λ_0 in $\mathbb{R}^m$ that is the intersection of the rational points of the modules $\Lambda_0(p)$:*

$$\Lambda_0 = \bigcap_{p \in \mathbb{P}} (\mathbb{Q}^m \cap \Lambda_0(p)).$$

Moreover,

$$\det \Lambda_0 = \prod_{p \in \mathbb{P}} [\mathbb{Z}_p^m : \Lambda_0(p)] \geq \prod_{p \in \mathbb{P}} \{\max_{v|p} |\mathcal{A}_v|_v\}_p.$$

Following the strategy adopted for a fixed prime p, we now apply the results of Theorem 4.4 to our problem. We will need:

Definition 4.5. To each $(\mathbf{A}, \mathbf{B}) \in \mathbb{Q}^{2n}$ with $|l_1^{i_1} \ldots l_m^{i_m}|_v \leq 1$ for all $v \in M_0(K)$, we associate the quantity $\mathbf{z} \in \prod_{p \in \mathbb{P}} (4m^3)^{-1} \mathbb{N}_0$ defined by

$$\mathbf{z}(\mathbf{A}, \mathbf{B}) := (z^{(p)}(\mathbf{A}, \mathbf{B}))_{p \in \mathbb{P}},$$

where $z^{(p)}(\mathbf{A}, \mathbf{B})$ is as in Definition 4.2.

As the reader may easily check, for given $(\mathbf{A}, \mathbf{B})$ there are only finitely many components of $\mathbf{z}(\mathbf{A}, \mathbf{B})$ different from 0; we denote their number by $r(\mathbf{z}) := r(\mathbf{z})(\mathbf{A}, \mathbf{B})$ and we are reduced to considering $\mathbf{z} \in \bigoplus_{p \in \mathbb{P}} (4m^3)^{-1} \mathbb{N}_0$ so that the expression $\prod_{p \in \mathbb{P}} c_1(m) z^{(p)} = c_1(m)^{r(\mathbf{z})} \prod_{p \in \mathbb{P}} z^{(p)}$ is well defined. This implies that the matrices $\mathcal{A}_v$ fall under the hypotheses of Theorem 4.4 and we find:

Corollary 4.6. *For given $\mathbf{z}$, the n-tuples $(\mathbf{A}, \mathbf{B})$ of pairs $(A_i, B_i) \in \mathbb{Q}^2$ of rational numbers satisfying $\mathbf{z}(\mathbf{A}, \mathbf{B}) = \mathbf{z} = (z^{(p)})_{p \in \mathbb{P}}$ lie in the union of $c_1(m)^{r(\mathbf{z})} \prod_{p \in \mathbb{P}} z^{(p)}$ lattices Λ of $\mathbb{R}^{2n}$ for which $\Lambda = \Lambda_0^n$, where Λ_0 is a lattice in $\mathbb{R}^2$ with*

$$\det \Lambda_0 \geq \prod_{p \in \mathbb{P}} \{|2m|_p |\Delta|_p^{1/(2m)} p^{z^{(p)}}\}_p.$$

Proof. By assumption $\mathbf{z}(\mathbf{A}, \mathbf{B}) = \mathbf{z} = (z^{(p)})_{p \in \mathbb{P}}$ and $z^{(p)} = 0$ for almost all $p \in \mathbb{P}$, so that $\mathcal{A}_v$ reduces to L_{j_0, j_1} for $v \,|\, p$ in this case. If in addition to $z^{(p)} = 0$ we also have $p \nmid 2m\Delta$, we obtain $|\mathcal{A}_v|_v = |\mathcal{A}_v|_v^{-1} = 1$, which yields $|\mathcal{A}_v \mathbf{X}|_v \leq 1 \Leftrightarrow |\mathbf{X}| \leq 1$, as required for the application of Theorem 4.4. Trivially, for $z^{(p)} = 0$ and fixed p, all solutions $\mathbf{X} = (A_i, B_i)$ of $|\mathcal{A}_v \mathbf{X}|_v \leq 1$ lie in one single $\mathbb{Z}_p$-module $\Lambda_0(p)$ of determinant $\geq \{|2m|_p|\Delta|_p^{1/(2m)}\}_p$, whereas for $z^{(p)} \neq 0$, Corollary 4.3 yields $c_1(m)z^{(p)}$ $\mathbb{Z}_p$-modules of determinant $\geq \{|2m|_p|\Delta|_p^{1/(2m)}p^{z^{(p)}}\}_p$.

Consequently, we have $c_1(m)^{r(\mathbf{z})}\prod_{p\in\mathbb{P}} z^{(p)}$ cases in which we may apply Theorem 4.4 to find that many lattices Λ_0 in $\mathbb{R}^2$ in which the (A_i, B_i) lie, whose determinant is bounded from below by

$$\prod_{p\in\mathbb{P}}\{|2m|_p|\Delta|_p^{1/(2m)}p^{z^{(p)}}\}_p.$$

Unfortunately this estimate may be too weak for those primes for which $|2m|_p|\Delta|_p^{1/(2m)}$ can be small, that is, for the divisors of $2m$ and Δ. That is where the role of the chosen system Π_d in which (λ, λ') lies becomes obvious. Since only primes p lying below the h prime ideals $\wp_1, \ldots, \wp_h$ that were chosen as representatives for the ideal classes of $\mathbb{Q}(\sqrt{d})$ may appear in mth power in Δ, we can expect to get a sufficiently decent bound for all but finitely many primes.

We consider a partition of $\mathbb{P}$ into 3 sets: P_1, P_2, P_3, where

$$P_1 = \{p \in \mathbb{P} : p \,|\, 2m \text{ or } \wp_j \,|\, p \text{ for some } 1 \leq j \leq h\}.$$

Note that P_1 is finite for each d independently of (λ, λ') and moreover, for given $(\lambda, \lambda') \in \Pi_d$ there is just one prime p_0 lying below the ideal class containing the mth power part of λ and λ'. We thus do not have to worry about the estimate of the index of $\Lambda_0(p)$ in this exceptional case. Next, we set

$$P_2 = \{p \in \mathbb{P} : p \,|\, \Delta,\ p \notin P_1\}.$$

The set P_2 is finite for any fixed $(\lambda, \lambda') \in \Pi_d$; it is for the primes in this set that the estimate of the index of $\Lambda_0(p)$ will have to be improved so as to allow a summation over all (λ, λ') in a fixed field $\mathbb{Q}(\sqrt{d})$. Finally, set

$$P_3 = \{p \in \mathbb{P} : p \notin (P_1 \cup P_2)\} = \{p \in \mathbb{P} : p \nmid 2m\Delta\}.$$

This set causes no problems since $|2m|_p|\Delta|_p^{1/(2m)} = 1$ in this case.

Proposition 4.7. *In the case $p \in P_2$ the estimate for the index of $\Lambda_0(p)$ in $\mathbb{Z}_p^2$ from Corollary* 4.3 *can be replaced by*

$$[\mathbb{Z}_p^2 : \Lambda_0(p)] \geq |\Delta|_p^{1/(2m)}p^{\max\{z^{(p)},1/(2m)\}}.$$

Proof. Since trivially $\{|\Delta|_p^{1/(2m)}p^{z^{(p)}}\}_p \geq |\Delta|_p^{1/(2m)}p^{z^{(p)}}$ by definition of $\{\ \}_p$, the statement of the proposition is surely true for $z^{(p)} \geq 1/(2m)$. Now assume $z^{(p)} < 1/(2m)$ as well as $p \,|\, \Delta$ and $p \notin P_1$. If $p^s \,\|\, \Delta$ (i.e. p^s is the greatest power of p dividing Δ) with $s \not\equiv 0 \pmod{2m}$, then $|\Delta|_p^{1/(2m)} \notin \{p^\nu : \nu \in \mathbb{Z}\}$ and the presence of $\{\ \}_p$ makes us gain at least $p^{1/(2m)}$, which leads to

$$\{|\Delta|_p^{1/(2m)}p^{z^{(p)}}\}_p \geq |\Delta|_p^{1/(2m)}p^{1/(2m)}.$$

We are thus left with the case $p^s \,\|\, \Delta$ for some $s \equiv 0 \pmod{2m}$. We claim $s = 2m$. Obviously $s > 0$ since $p \mid \Delta$. If we had $p^{4m} \mid \Delta$, we would get $p^{4m} \mid d^m(\lambda\lambda')^2$ by definition of Δ and further

$$p \nmid d \;\Rightarrow\; p^{2m} \mid \lambda\lambda' \;\Rightarrow\; \exists \pi \mid p : \pi^m \mid \lambda,\, \pi^m \mid \lambda' \;\Rightarrow\; p = p_0,$$

$$p \mid d \;\Rightarrow\; p^{3m} \mid (\lambda\lambda')^2 \text{ and } p = \pi^2 \;\Rightarrow\; \pi^{3m} \mid \lambda\lambda' \;\Rightarrow\; \pi^m \mid \lambda,\, \pi^m \mid \lambda' \;\Rightarrow\; p = p_0,$$

a contradiction to $p \neq p_0$ in both cases.

So we only have to consider the case $|\Delta|_p = p^{2m}$, where we will show that $z^{(p)}(\mathbf{A}, \mathbf{B}) = z^{(p)} < 1/(2m)$ and $p^{2m} \,\|\, \Delta$ already imply $(\mathbf{A}, \mathbf{B}) \in \mathbb{Z}_p^{2n}$ and

$$[\mathbb{Z}_p^2 : \Lambda_0(p)] \geq 1 = |\Delta|_p^{1/(2m)}p > |\Delta|_p^{1/(2m)}p^{1/(2m)}$$

will prove the assertion.

Note that $p^{2m} \,\|\, \Delta$ yields $p^{2m} \,\|\, d^m(\lambda\lambda')^2$, hence for

$$p \mid d \;\Rightarrow\; (p) = \pi^2,\, \pi^{4m} \,\|\, d^m(\lambda\lambda')^2 \;\Rightarrow\; \pi^m \,\|\, \lambda\lambda' \;\Rightarrow\; p \mid \lambda \text{ and } p \mid \lambda'$$

for $m \geq 4$ since $p \mid d \Rightarrow m \neq 3$, and

$$p \nmid d,\, d = 1 \;\Rightarrow\; p^{2m} \mid (\lambda\lambda')^2 \;\Rightarrow p^m \mid \lambda\lambda' \;\Rightarrow\; p \mid \lambda \text{ and } p \mid \lambda',$$

$$p \nmid d,\, d \neq 1 \;\Rightarrow\; (p) = \pi\pi',\, (\pi\pi')^m \,\|\, \lambda\lambda' \;\Rightarrow\; \pi\pi' \mid \lambda,\, \pi\pi' \mid \lambda' \;\Rightarrow\; p \mid \lambda,\, p \mid \lambda',$$

since $p \neq p_0$ by assumption.

Altogether every valuation $v \mid p$ has

$$|\lambda|_v \leq p^{-1} \quad \text{and} \quad |\lambda'|_v \leq p^{-1};$$

the entries of L_{j_0,j_1} being linear combinations of $\lambda^{1/m}, {\lambda'}^{1/m}$ with integral coefficients, this implies $|L_{j_0,j_1}|_v \leq p^{-1/m}$.

Now, by Theorem 4.1 (see notation there)

$$|\mathcal{A}_v\mathbf{x}|_v \leq 1 \;\Rightarrow\; |\mathbf{X}|_v \leq |\mathcal{A}_v^{-1}|_v \leq |\mathcal{A}_v|_v |\det \mathcal{A}_v|_v^{-1}.$$

Plugging in, we find

$$|\det \mathcal{A}_v|_v \geq p^{z^{(p)}}|\Delta|_p^{1/(2m)} = p^{z^{(p)}-1}$$

and

$$|\mathcal{A}_v|_v = p^{-z_{j_0}^{(v)}}|L_{j_0,j_1}|_v \leq p^{-z_{j_0}^{(v)}}p^{-1/m}.$$

As already seen $-z_{j_0}^{(v)} \leq \frac{m-1}{m-2}z^{(p)}$ and we conclude

$$|\mathcal{A}_v|_v \leq p^{\frac{m-1}{m-2}z^{(p)}}p^{-1/m}.$$

In combination with the estimate of $|\det \mathcal{A}_v|_v$ this yields

$$|\mathbf{X}|_v \leq p^{-z^{(p)}+1}p^{\frac{m-1}{m-2}z^{(p)}-1/m} = p^{\frac{z^{(p)}}{m-2}+\frac{m-1}{m}} < p \quad \text{for } m \geq 3$$

since $z^{(p)}$ was supposed $< 1/(2m)$ and everything is proved.

5. The synthesis of both problems. It is now time to recombine the archimedean and non-archimedean parts of the problem, that is, to establish a relation between points in the lattices Λ and those in the domain $S(X)$. The appropriate context for this purpose is the two-dimensional level, i.e. the centrally symmetric, convex sets $P_s^{(k)}$and the lattices Λ_0. For this lattice point count, we refer to a result from the geometry of numbers:

Proposition 5.1. *Let Λ denote a lattice in $\mathbb{R}^2$ and K a convex set in $\mathbb{R}^2$ that is symmetric with respect to the origin and has volume $V(K)$. Then the number of n-tuples $(\mathbf{g}_1,\ldots,\mathbf{g}_n)$ with $\mathbf{g}_i\in\Lambda\cap K$ for $i=1,\ldots,n$ for which $\mathbf{g}_1,\ldots,\mathbf{g}_n$ span $\mathbb{R}^2$ is $\ll (V(K)/\det\Lambda)^n$, with the implied constant depending on n only.*

Proof. See [Su] for the details of this special case or [G-L] and [Sch] for reference.

In the present situation, we have to deal with $c_1(m)^{r(\mathbf{z})}\prod_{p\in\mathbb{P}}z^{(p)}$ lattices $\Lambda_0=\Lambda_0(\mathbf{z})$ for given $\mathbf{z}$ and m possible covering sets $P^{(k)}$ for given k and we write $\mathbf{z}^*(\mathbf{A},\mathbf{B})=(k,\mathbf{z})$ for those $(\mathbf{A},\mathbf{B})$ whose components lie in the intersection of one of the above lattices with one of the covering sets and abbreviate $c_1:=c_1(m)$.

Corollary 5.2. *The number of n-tuples $(\mathbf{A},\mathbf{B})$ of pairs $(A_i,B_i)\in\mathbb{Q}^2$ satisfying $\mathbf{z}^*(\mathbf{A},\mathbf{B})=(k,\mathbf{z})$ for which $(A_1,B_1),\ldots,(A_n,B_n)$ span $\mathbb{R}^2$ is*

$$\ll X^{2n/m}c_1^{r(\mathbf{z})}\prod_{p\in\mathbb{P}}z^{(p)}\Big[2^{nk}\prod_{p\in P_1}p^{nz^{(p)}}\prod_{p\in P_3}\{p^{nz^{(p)}}\}_p\prod_{p\in P_2}p^{n\max\{1/(2m),z^{(p)}\}}\Big]^{-1},$$

if we set $\prod_{p\in\mathbb{P}}z^{(p)}=1$ whenever $z^{(p)}=0$ for all p.

Proof. By assumption $\mathbf{z}(\mathbf{A},\mathbf{B})=\mathbf{z}$ and the $(\mathbf{A},\mathbf{B})$ in question lie in one of $c_1^{r(\mathbf{z})}\prod_{p\in\mathbb{P}}z^{(p)}$ lattices Λ_0 with

$$\det\Lambda_0\ge\prod_{p\in\mathbb{P}}\{|2m|_p|\Delta|_p^{1/(2m)}p^{z^{(p)}}\}_p.$$

Moreover all components of $(\mathbf{A},\mathbf{B})$ lie in one of the m covering sets $P_s^{(k)}$, each of which is convex, symmetric with respect to the origin in $\mathbb{R}^2$ with volume

$$V(P_s^{(k)})\ll 2^{-k}|\Delta|_\infty^{-1/(2m)}X^{2/m}.$$

Thus for a fixed lattice Λ_0 and a given set $P_s^{(k)}$ the conditions of Proposition 5.1 are fulfilled and in $(V(K)/\det\Lambda)^n$ the main term $X^{2n/m}$ has a factor

$$\Big(2^k|\Delta|_\infty^{1/(2m)}\prod_{p\in P_1\cup P_3}\{|2m|_p|\Delta|_p^{1/(2m)}p^{z^{(p)}}\}_p\prod_{p\in P_2}|\Delta|_p^{1/(2m)}p^{\max\{1/(2m),z^{(p)}\}}\Big)^{-n}.$$

For $p \in P_1$ we use the trivial estimate

$$\{|2m|_p|\Delta|_p^{1/(2m)}p^{z^{(p)}}\}_p \geq |2m|_p|\Delta|_p^{1/(2m)}p^{z^{(p)}} \gg |\Delta|_p^{1/(2m)}p^{z^{(p)}},$$

whereas for $p \in P_3$ we have $|2m|_p|\Delta|_p^{1/(2m)} = 1$, which leaves us with $\{p^{z^{(p)}}\}_p$ only.

By the product formula,

$$|\Delta|_\infty \prod_{p\in P_1} |\Delta|_p \prod_{p\in P_2} |\Delta|_p = \prod_{p\in \mathbb{P}\cup\infty} |\Delta|_p = 1$$

and the dependence on Δ cancels.

Finally, taking into account the number of possible lattices Λ_0, we easily get the desired result.

To get information about points $(\mathbf{A},\mathbf{B})$ in $S(X)$ that lie in the union of the lattices $\Lambda(\mathbf{z})$ for some $\mathbf{z}$, we have to sum over all $k \in \mathbb{N}$ and $\mathbf{z} = (z^{(p)})_{p\in\mathbb{P}}$ with $4m^3z^{(p)} \in \mathbb{Z}$ and $z^{(p)} = 0$ for almost all p. The summation over k is straightforward since $\sum_{k\in\mathbb{N}} 2^{-k} \ll 1$; for the one over $\mathbf{z}$ we need some technical details, most of which may be left to the reader:

Lemma 5.3. *The following estimates hold with positive constants* $c_0(m)$, $c_2(m)$, $c_3(m)$ *that depend on* m *only and will be abbreviated as* c_0, c_2, c_3:

$$\prod_{p\in P_1}\Big(1+\sum_{s=1}^{\infty} c_1(m)\frac{s}{4m^3}p^{(-ns)/(4m^3)}\Big) \ll c_2(m)h(d),$$

$$\prod_{p\in P_3}\Big(1+\sum_{s=1}^{\infty} c_1(m)\frac{s}{4m^3}p^{n[-s/(4m^3)]}\Big) \ll c_3(m),$$

$$\prod_{p\in P_2}\Big(\sum_{s=0}^{\infty} c_1(m)\frac{s}{4m^3}p^{-n\max(1/(2m),s/(4m^3))}\Big) \ll c_0(m)^{|P_2|}\prod_{p\in P_2} p^{-n/(2m)}.$$

Proof. The following estimate is obtained by elementary calculus:

$$\sum_{s=1}^{\infty} sp^{-ns} \ll \int_1^{\infty} sp^{-ns}\,ds \ll p^{-n}$$

and the first assertion follows immediately since $|P_1| \ll h(d)$ by construction. For the second one, we observe that only integer powers of p may appear for $p \in P_3$, so that

$$\prod_{p\in P_3}\Big(1+\sum_{s=1}^{\infty} c_1\frac{s}{4m^3}p^{n[-s/(4m^3)]}\Big) = \prod_{p\in P_3}\Big(1+c_1\sum_{s=1}^{\infty} sp^{-ns}\Big) \ll \prod_{p\in P_3}(1+c_1p^{-n}),$$

and extending the last product over all primes yields

$$\prod_{p\in\mathbb{P}}(1+c_1p^{-n}) \ll \sum_s c_1^{\omega(s)}s^{-n} \ll c_2(m)$$

for $n \geq 2$, if we use the well known estimate $\omega(s) \ll \log s (\log\log s)^{-1}$ which readily implies $a^{\omega(s)} \ll s^{\varepsilon}$ for any $\varepsilon > 0$ and any fixed parameter a. For the third product, we split up the sum involved in two parts, namely for $0 \leq s \leq 2m^2 - 1$ and $s \geq 2m^2$ so that $\max(1/(2m), s/(4m^3)) = 1/(2m)$ respectively $s/(4m^3)$ to obtain

$$\begin{aligned}
&\prod_{p\in P_2}\Big(\sum_{s=0}^{\infty} c_1 \frac{s}{4m^3} p^{-n\max(1/(2m),s/(4m^3))}\Big)\\
&\qquad = \prod_{p\in P_2}\Big(\sum_{s=0}^{2m^2-1} c_1 \frac{s}{4m^3} p^{-n/(2m)} + \sum_{s=2m^2}^{\infty} c_1 \frac{s}{4m^3} p^{(-ns)/(4m^3)}\Big)\\
&\qquad \ll \prod_{p\in P_2} (c_1' p^{-n/(2m)} + c_1'' p^{-n/(2m)})\\
&\qquad \ll c_0(m)^{|P_2|} \prod_{p\in P_2} p^{-n/(2m)},
\end{aligned}$$

for suitable constants c_1', c_1'', c_0 depending on m only.

Proposition 5.4. *The number of n-tuples $(\mathbf{A},\mathbf{B}) = (A_i, B_i)_{i=1,\ldots,n}$ of pairs $(A_i, B_i) \in \mathbb{Q}^2$ for which $(A_1, B_1), \ldots, (A_n, B_n)$ span $\mathbb{R}^2$ and which lie in the union over $k \in \mathbb{N}$ and $\mathbf{z} \in \bigoplus_{p\in\mathbb{P}} (4m^3)^{-1}\mathbb{N}_0$ of the intersections of $P^{(k)}$ with one of the lattices $\Lambda(\mathbf{z})$ is*

$$\ll X^{2n/m} h(d)\Big(c_0^{|P_2|} \prod_{p\in P_2} p^{-n/(2m)}\Big).$$

Proof. The n-tuples $(\mathbf{A},\mathbf{B})$ in question are precisely those treated in Corollary 5.2 for a given $\mathbf{z}^* = (k, \mathbf{z})$. Thus we have to sum over the $(\mathbf{A},\mathbf{B})$ in this estimate over all parameters k and $\mathbf{z}$. In

$$\sum_{k\in\mathbb{N}}\sum_{\mathbf{z}} c_1^{r(\mathbf{z})} 2^{-nk} \prod_{p\in P_1} z^{(p)} p^{-nz^{(p)}} \prod_{p\in P_3} z^{(p)} \{p^{-nz^{(p)}}\}_p \prod_{p\in P_2} z^{(p)} p^{-n\max\{1/(2m),z^{(p)}\}}$$

we may take the sum over k and use the identity

$$\sum_{\mathbf{z}} c_1^{r(\mathbf{z})} \prod_{p\in\mathbb{P}} p^{\nu_p(z^{(p)})} = \prod_{p\in\mathbb{P}} \Big(p^{\nu_p(0)} + c_1 \sum_{z^{(p)}} p^{\nu_p(z^{(p)})}\Big),$$

with $\nu_p(z^{(p)})$ being one of the above exponents. This leads to

$$\begin{aligned}
\prod_{p\in P_1}\Big(1 + \sum_{s=1}^{\infty} c_1 \frac{s}{4m^3} p^{(-ns)/(4m^3)}\Big) \prod_{p\in P_3}\Big(1 + \sum_{s=1}^{\infty} c_1 \frac{s}{4m^3} p^{n[-s/(4m^3)]}\Big)&\\
\times \prod_{p\in P_2}\Big(\sum_{s=0}^{\infty} c_1 \frac{s}{4m^3} p^{-n\max(1/(2m),s/(4m^3))}\Big)&,
\end{aligned}$$

and those factors were estimated in Lemma 5.3 to give the predicted result.

To determine the order of magnitude of $Z((\lambda,\lambda'),d,n,m,X)$, it only remains to show that the n-tuples $(\mathbf{A},\mathbf{B})$ counted there are among the ones Proposition 5.4 deals with.

This requires two steps. On the one hand, the condition that $(A_i,B_i)_{i=1,\dots,n}$ span $\mathbb{R}^2$ means precisely that those n-tuples lead to non-degenerate forms. On the other hand, $(\mathbf{A},\mathbf{B})\in S(X)\subset\bigcup_{k=1}^{\infty}\bigcup_{s=1}^{m}(P_s^{(k)})^n$ and $(\mathbf{A},\mathbf{B})\in\bigcup_{\mathbf{z}}\mathit{\Lambda}(\mathbf{z})$ so that they fall under the conditions of the proposition. We have thus proved:

Theorem 5.5. *For $(\lambda,\lambda')\in\mathit{\Pi}_d$ and $n\ge 2$ we have*

$$Z((\lambda,\lambda'),d,n,m,X)\ll X^{2n/m}h(d)\Big(c_0^{|P_2|}\prod_{p\in P_2}p^{-n/(2m)}\Big),$$

where the constant in $\ll$ depends on n and m only, in particular it is independent of (λ,λ') and d.

We are now in a position to estimate $\sum_{(\lambda,\lambda')\in\mathit{\Pi}_d}Z((\lambda,\lambda'),d,n,m,X)$ as was outlined in Section 1 to get the desired bound on $Z(d,n,m,X)$.

In order to bring into evidence the dependence on (λ,λ') of the summands on the right, we note that $|P_2|\le\omega(d)+\omega(\lambda\lambda')$ and summarizing the conditions $p\,|\,\lambda\lambda', p\nmid d$ and $p\ne p_0$ by $p\in T(\lambda\lambda')$ gives

$$\prod_{p\in P_2}p^{-n/(2m)}\ll|d|^{-n/(2m)}\prod_{p\in T(\lambda\lambda')}p^{-n/(2m)},$$

and we obtain

$$Z((\lambda,\lambda'),d,n,m,X)\ll X^{2n/m}h(d)c_0^{\omega(d)}|d|^{-n/(2m)}c_0^{\omega(\lambda\lambda')}\prod_{p\in T(\lambda\lambda')}p^{-n/(2m)}.$$

Let us keep the prime p_0 and thus the ideal class of the mth power part of λ fixed to deal with the expression

$$\sum_{(\lambda\lambda')\in\mathit{\Pi}_d(p_0)}c_0^{\omega(\lambda\lambda')}\prod_{p\in T(\lambda\lambda')}p^{-n/(2m)},$$

where $\mathit{\Pi}_d(p_0)$ abbreviates the above restriction on (λ,λ'). Note that each summand depends only on $N:=\mathcal{N}(\lambda)=\lambda\lambda'$, so we get:

Proposition 5.6. *Let $(\lambda,\lambda')\in\mathit{\Pi}_d$ with $(\lambda)=\wp_0^m a$ where $\wp_0\,|\,p_0$ is some fixed prime ideal from $\{\wp_1,\dots,\wp_h\}$. Then the exponent of each prime divisor of $N:=\mathcal{N}(\lambda)=\lambda\lambda'$ is bounded by a constant ϕ_m that depends on m only and there are at most $m^{\omega(N)}$ ideals of the form $(\lambda)=\wp_0^m a$ with $\mathcal{N}(\lambda)=N$. In particular, $p_0^m\,|\,N$.*

Proof. Since $(\lambda)=\wp_0^m a=\wp_0^{e_0}\prod\varrho_i^{e_i}$ where a is assumed to be free of mth powers, the first statement of the proposition becomes obvious if we note that $m\le e_0\le 2m-1$ and $e_i\le m-1$ for $i\ge 0$. Turning to the statement concerning the number of ideals that have norm N, we assume $N = p_0^{s_0} p_1^{s_1} \dots p_r^{s_r}$. If a prime p_i does not split in $\mathbb{Q}(\sqrt{d})$, its exponent is already determined by e_i, whereas when p_i splits, there are only m possible choices for the exponent of each of its two factors in the decomposition of (λ) since the possible exponents are between 0 and $m-1$ for $i \geq 0$ and between m and $2m-1$ for $i = 0$. Thus there are at most $m^{\omega(N)}$ ideals of the form $(\lambda) = \wp_0^m a$ with given norm N.

Proposition 5.7. *Let M denote the square-free part of $N = \mathcal{N}(\lambda)$, $\tau := (M,d)$ und $L := M/\tau$. Then there is a constant $C_0 > 0$, depending on m only, for which*

$$\sum_{(\lambda\lambda') \in \Pi_d(p_0)} c_0^{\omega(N)} \prod_{p \in T(N)} p^{-n/(2m)} \ll C_0^{\omega(d)} \Big(\sum_{L=1}^{\infty} C_0^{\omega(L)} L^{-n/(2m)} \Big).$$

Proof. By Proposition 5.6 we have

$$\sum_{(\lambda\lambda') \in \Pi_d(p_0)} c_0^{\omega(\lambda\lambda')} \prod_{p \in T(\lambda\lambda')} p^{-n/(2m)} \ll \sum_{N \in \Phi} (mc_0)^{\omega(N)} \prod_{p \in T(N)} p^{-n/(2m)},$$

where Φ denotes the set of integers whose prime factors all have exponents $\leq \phi_m$. In the right hand sum, the summand depends on the square-free part M of N only ($\Rightarrow \omega(N) = \omega(M)$) and since N is free of ϕ_mth powers, we may write

$$\sum_{N \in \Phi} (mc_0)^{\omega(N)} \prod_{p \in T(N)} p^{-n/(2m)} \ll \sum_{M \text{ sq-free}} (\phi_m m c_0)^{\omega(M)} \prod_{p \in T(M)} p^{-n/(2m)}.$$

If we keep $(M,d) := \tau$ fixed, we have $p_0 \nmid \tau$ by assumption since $(p_0, d) = 1$ and we obtain

$$\prod_{p \in T(M)} p^{-n/(2m)} = (M/\tau)^{-n/(2m)} \qquad \text{for } p_0 \nmid M,$$

$$\prod_{p \in T(M)} p^{-n/(2m)} = (M/p_0\tau)^{-n/(2m)} \qquad \text{for } p_0 \mid M.$$

This implies further

$$\sum_{\substack{(M,d)=\tau \\ M \text{ sq-free}}}^{\infty} (\phi_m c_0)^{\omega(M)} \prod_{p \in T(M)} p^{-n/(2m)}$$

$$\leq \sum_{\substack{(M,d)=\tau \\ (M,p_0)=1 \\ M \text{ sq-free}}}^{\infty} (\phi_m c_0)^{\omega(M)} (M/\tau)^{-n/(2m)} + \sum_{\substack{(M,d)=\tau \\ p_0 \mid M \\ M \text{ sq-free}}}^{\infty} (\phi_m c_0)^{\omega(M)} (M/p_0\tau)^{-n/(2m)}.$$

Both sums differ by a factor that depends on m only, so

$$\sum_{\substack{(M,d)=\tau\\ M \text{ sq-free}}} (\phi_m c_0)^{\omega(M)} \prod_{p\in T(M)} p^{-n/(2m)} \ll \sum_{\substack{(M,d)=\tau\\ M \text{ sq-free}}} (\phi_m c_0)^{\omega(M)} (M/\tau)^{-n/(2m)}.$$

With $M/\tau = L$ we get $\omega(M) = \omega(L) + \omega(\tau)$ and summation over all divisors τ of d gives (dropping the condition M sq-free)

$$\sum_{\tau\mid d}\Big(\sum_{(M,d)=\tau}^{\infty} (\phi_m c_0)^{\omega(M)} (M/\tau)^{-n/(2m)}\Big)$$
$$= \sum_{\tau\mid d} (\phi_m c_0)^{\omega(\tau)} \Big(\sum_{L=1}^{\infty} (\phi_m c_0)^{\omega(L)} L^{-n/(2m)}\Big).$$

The number of $\tau \mid d$ with $\omega(\tau) = j$ is precisely $\binom{\omega(d)}{j}$, and thus we find

$$\sum_{\tau\mid d} (\phi_m c_0)^{\omega(\tau)} = \sum_{j=0}^{\omega(d)} \binom{\omega(d)}{j} (\phi_m c_0)^j = (\phi_m c_0 + 1)^{\omega(d)} =: C_0^{\omega(d)}$$

by the binomial theorem, which concludes the proof.

At this stage, we need a restriction on n that guarantees the convergence of $\sum_{L=1}^{\infty} C_0^{\omega(L)} L^{-n/(2m)}$ to prove the final step in our deduction, namely Theorem 1.4 already stated in Section 1.

Theorem 5.8. *Let $n > 2m$ and $h = h(d)$ be the class number of the quadratic field $\mathbb{Q}(\sqrt{d})$. Then there exists a constant $C > 0$ that depends on m only with*

$$Z(d, n, m, X) \ll X^{2n/d} h^2(d) C^{\omega(d)} |d|^{-n/(2m)},$$

with the constant in $\ll$ depending on n and m.

Proof. As already seen, we have

$$Z(d, n, m, X)$$
$$= \sum_{(\lambda,\lambda')\in\Pi_d} Z((\lambda,\lambda'), d, n, m, X)$$
$$\ll X^{2n/m} h(d) \sum_{p_0\in\{p_1,\dots,p_h\}} \Big(\sum_{(\lambda,\lambda')\in\Pi_d(p_0)} c_0^{\omega(\lambda\lambda')} \prod_{p\in T(\lambda\lambda')} p^{-n/(2m)}\Big) c_0^{\omega(d)} |d|^{-n/(2m)}$$
$$\ll X^{2n/m} h^2(d) \Big(C_0^{\omega(d)} \Big(\sum_{L=1}^{\infty} C_0^{\omega(L)} L^{-n/(2m)}\Big)\Big) c_0^{\omega(d)} |d|^{-n/(2m)}$$

by Theorem 5.5 and Proposition 5.7. The estimate

$$\omega(L) \ll \log L (\log\log L)^{-1} \;\Rightarrow\; (C_0)^{\omega(L)} \ll L^{\varepsilon}$$

for any $\varepsilon > 0$ with the constant in $\ll$ depending on m, ε then implies

$$\sum_{L=1}^{\infty} C_0^{\omega(L)} L^{-n/(2m)} \ll 1$$

for $n > 2m$. Putting $C := c_0 C_0$ leads to

$$Z(d,n,m,X) \ll X^{2n/d} h^2(d) C^{\omega(d)} |d|^{-n/(2m)},$$

and the proof is complete.

References

[E-K] A. Eskin and Y. R. Katznelson, *Singular symmetric matrices*, Duke Math. J. 79 (1995), 515–547.

[G-L] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers*, North Holland, 1987.

[K] Y. R. Katznelson, *Integral matrices of fixed rank*, Proc. Amer. Math. Soc. 120 (1994), 667–675.

[La] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[NRRL] N. Narasimhan, S. Raghavan, S. Rangachari and S. Lal, *Algebraic Number Theory*, Tata Institute, Bombay, 1966.

[N] J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1993.

[Sch] W. M. Schmidt, *Northcott's theorem on heights II. The quadratic case*, Acta Arith. 70 (1995), 343–375.

[Su] L. Summerer, *Cubic forms as sum of cubes of linear forms*, J. Number Theory 73 (1998), 472–517.

Institute of Mathematics
University of Vienna
Strudlhofgasse 4
A-1090 Wien, Austria
E-mail: leonhard.summerer@univie.ac.at

Received on 24.3.1999
and in revised form on 12.7.2001 (3577)