ACTA ARITHMETICA
LXXIX.2 (1997)

Counting solutions of decomposable form equations

by

G. R. Everest (Norwich) and K. Győry (Debrecen)

To Professor J. W. S. Cassels on his 75th birthday

1. Introduction. Let M be a number field, $L(\mathbf{x}) = \alpha_1 x_1 + \ldots + \alpha_n x_n$ a linear form with linearly independent coefficients in M, $c \in \mathbb{Q}^*$ (1) and $a \in \mathbb{Z} - \{0\}$. By means of his Subspace Theorem, Schmidt [11] showed that the solutions $\mathbf{x} \in \mathbb{Z}^n$ of the norm form equation

$$cN_{M|\mathbb{Q}}(L(\mathbf{x})) = a \tag{1.1}$$

belong to a finite number of so-called families of solutions (cf. Section 2). Let $P(N)$ denote the number of solutions $\mathbf{x}$ of (1.1) with $|\mathbf{x}| = \max_{1\le i\le n}\{|x_i|\} < N$. Using this result of Schmidt, Győry and Pethő [8] proved that if (1.1) has infinitely many solutions then

$$P(N) = \varrho_1(\log N)^r + O((\log N)^{r-1}) \quad \text{as } N \to \infty, \tag{1.2}$$

with a positive constant ϱ_1. In (1.2), r denotes a positive integer which, in the language of Section 2, denotes the maximum of the unit ranks of those subfields of M to which there corresponds a family of solutions. When $n = [M : \mathbb{Q}]$, we say the form is *full* and in this case, Győry and Pethő [9] gave explicitly the constant ϱ_1 together with an explicit bound for the constant implied by the O notation. Later, Everest [3], refined the result in [9], in the case where M is totally real and $r > 1$, to deduce

$$P(N) = \varrho_1(\log N)^r + \varrho_2(\log N)^{r-1} + o((\log N)^{r-1}) \quad \text{as } N \to \infty. \tag{1.3}$$

Further, he gave the constant ϱ_2 in an explicit form. It is interesting to compare the dependence of the constants ϱ_1 and ϱ_2 upon F and a. The

The research of the second author was partially supported by the Hungarian Academy of Sciences and by the Hungarian National Foundation for Scientific Research, Grants No. 16975 and 16791.

(1) For a ring R with unity, R^* will denote the multiplicative group of invertible elements of R.

dependence of ϱ_1 upon a is marginal having to do with the number of maximal families of solutions. Also ϱ_1 contains a transcendental part, a rational multiple of the inverse regulator of M. The dependence of ϱ_2 upon a and F is more subtle. In [2], the first author gave an approach to the explicit determination of these constants using Dirichlet's series.

The purpose of this paper is to generalise the result of [8] to arbitrary decomposable form equations over $\mathbb{Z}$ (see Theorem 1) and the result of [3] to a general class of such equations (see Theorem 2). Further, we give a surprising application to the distribution of units in abelian group rings (see Theorem 3). The constants ϱ_1 and ϱ_2 are ineffective since our proof depends upon the Thue–Siegel–Roth–Schmidt method. We intend to provide explicit formulae for these constants in our next paper, in the case where $n = \deg F$, using the methods of [9], [2] and [3]. This will yield explicit constants in Theorem 3 also.

Let $F(\mathbf{x}) = F(x_1, \ldots, x_n)$ denote a decomposable form with coefficients in $\mathbb{Z}$. That is, $F(\mathbf{x})$ is a homogeneous polynomial which factorises into linear factors with algebraic coefficients. Then there are $c \in \mathbb{Q}^*$, finite extension fields $M_1, \ldots, M_t$ of $\mathbb{Q}$ and linear forms $L_i(\mathbf{x})$ with coefficients in $M_i, i = 1, \ldots, t$, such that

$$F(\mathbf{x}) = c \prod_{i=1}^{t} N_{M_i|\mathbb{Q}}(L_i(\mathbf{x})). \tag{1.4}$$

Assume that F has n linearly independent linear factors with algebraic coefficients and $a \in \mathbb{Z}$. The *decomposable form equation*

$$F(\mathbf{x}) = a, \quad \mathbf{x} \in \mathbb{Z}^n, \tag{1.5}$$

is a generalisation of the equation in (1.1). In [7], Győry extended the concept of family of solutions (cf. Section 2) to decomposable form equations, and showed that the solutions are all contained in the union of finitely many families of solutions. By means of this, Evertse and Győry [5] have obtained a formula like (1.2) for the solutions of a re-formulation of (1.5).

First we will prove a formula (1.2) (see Theorem 1) for the equation (1.5). This could be deduced directly from the finiteness results of [7]. However, it will be shorter to derive it from the formula in [5]. Further, by using the method of [3], we will generalise (1.3) (Theorem 2) for the equation (1.5) under restrictive hypotheses on the fields M_i. As an application, we will give asymptotic formulae (Theorem 3) counting units in group rings $\mathbb{Z}\Gamma$, where Γ denotes a finite abelian group.

We would like to point out that our methods give insight into the location in space of the solutions of the equation in (1.5). Suppose we project the solutions $\mathbf{x} \in \mathbb{Z}^n$ of (1.5) centrally onto the unit ball by dividing each one by its length. We might ask what is the distribution of the images. Our methods show that, far from being uniformly distributed, the images cluster more densely around a finite number of points on the ball. Say we were to imagine the solutions represented by stars in the sky and the origin at the earth's centre. Looking up into the night sky, what we would see, amongst the scattered lights, is a finite collection of brighter clusters of stars. These would be joined by less bright lines (like the "Milky Way"). This remark will be explained at the end of Section 5.

On this topic, the choice of Euclidean norm (in this case, the "max"-norm) used to compute $P(N)$ may seem a little arbitrary. Since any two norms are commensurate, it is easily seen that (1.2) is independent of the choice in the sense that only the constant implied by the O notation is affected by a change of norm. It is a more delicate matter to assess the dependence of ϱ_2 (in (1.3)) upon the choice of norm.

2. Results. Let $M_1, \ldots, M_t$ appear as before (see (1.4)) and let A denote the algebra

$$A = M_1 \oplus \ldots \oplus M_t.$$

This is the direct $\mathbb{Q}$-algebra sum of the algebraic number fields formed with respect to componentwise operations. Thus, $1_A = (1, \ldots, 1)$ is the unity of A and A^*, the multiplicative group of invertible elements of A is $\{(\alpha_1, \ldots, \alpha_t) \in A : \alpha_1 \ldots \alpha_t \neq 0\}$. The norm $N_{A|\mathbb{Q}}(\alpha)$ of $\alpha = (\alpha_1, \ldots, \alpha_t) \in A$ is defined to be the usual algebra norm, i.e. the determinant of the $\mathbb{Q}$-linear map $x \mapsto \alpha x$ from A to itself. The norm is multiplicative and we have

$$N_{A|\mathbb{Q}}(\alpha) = \prod_{i=1}^{t} N_{M_i|\mathbb{Q}}(\alpha_i). \tag{2.1}$$

In view of (1.4), we may re-write equation (1.5) as

$$cN_{A|\mathbb{Q}}(x) = a, \qquad x \in \mathfrak{M}, \tag{2.2}$$

where, in (2.2), $\mathfrak{M}$ is defined to be $\mathfrak{M} = \{x = (L_1(\mathbf{x}), \ldots, L_t(\mathbf{x})) \in A : \mathbf{x} \in \mathbb{Z}^n\}$. Now $\mathfrak{M}$ is a finitely generated $\mathbb{Z}$-module.

Following [7] and [5], we now define the concept of family of solutions. Let $V = \mathbb{Q}\mathfrak{M}$ denote the $\mathbb{Q}$-vector space generated by $\mathfrak{M}$. For any subalgebra B of A with $1_A \in B$, denote by O_B the integral closure of $\mathbb{Z}$ in B. Let

$$V^B = \{v \in V : vB \subseteq V\} \quad \text{and} \quad \mathfrak{M}^B = V^B \cap \mathfrak{M}.$$

Obviously V^B is closed under multiplication by elements of B. Now define

$$U_{\mathfrak{M},B} = \{\varepsilon \in O_B^* : \varepsilon\mathfrak{M}^B = \mathfrak{M}^B,\ N_{A|\mathbb{Q}}(\varepsilon) = 1\}.$$

This is a subgroup of finite index in O_B^* (see [7]). If $x \in \mathfrak{M}^B$ is a solution of (2.2) so is every element of $xU_{\mathfrak{M},B}$. Such a coset is called an $(\mathfrak{M}, B)$-*family* *of solutions* of (2.2), and hence of (1.5) as well. The group O_B^* is finitely generated; let r_B denote the torsion-free rank.

Theorem 1. *Suppose that equation* (1.5) *has infinitely many solutions. Let r denote the maximum of the ranks r_B, taken over all $\mathbb{Q}$-subalgebras B of A with $1_A \in B$, for which* (2.2) *has an $(\mathfrak{M}, B)$-family of solutions. Then the counting function $P(N)$ of equation* (1.5) *satisfies* (1.2), *with a positive constant ϱ_1 which depends only upon F and a.*

We will see that $r > 0$ precisely when (1.5) has infinitely many solutions.

In the special case where $t = 1$, equation (2.2) reduces to the equation

$$cN_{M_1|\mathbb{Q}}(x) = a, \qquad x \in \mathfrak{M}, \tag{2.3}$$

where now $\mathfrak{M} = \{x = L_1(\mathbf{x}) : \mathbf{x} \in \mathbb{Z}^n\}$. This is a re-formulation of equation (1.1). Theorem 1 applies to (2.3), replacing the subalgebras of A by subfields of M_1. Hence in this case, Theorem 1 gives the main result of [8], concerning equation (1.1).

Theorem 2. *Let r be as in Theorem* 1 *and assume that $r > 1$. Suppose that the number fields $M_1, \ldots, M_t$ associated with F in* (1.4) *have the following properties: they are totally real fields or totally imaginary quadratic extensions of totally real fields, they have unit ranks greater than* 1 *and none of them has a subfield of unit rank* 1. *Then the counting function $P(N)$ of equation* (1.5) *satisfies* (1.3) *with constants $\varrho_1 > 0$ and ϱ_2 which depend on F and a. If $n = \sum_{i=1}^t [M_i : \mathbb{Q}]$ then the condition on the subfields of $M_1, \ldots, M_t$ can be omitted.*

For the case where $t = 1$, $n = [M_1 : \mathbb{Q}]$ with M_1 totally real, Theorem 2 provides the main result of [3].

The following example shows that, in Theorem 2, the conditions imposed on the unit ranks of $M_1, \ldots, M_t$ and their subfields are necessary. For $i = 1, \ldots, t$, let d_i denote distinct, positive, square-free integers greater than 1, and let $M_i = \mathbb{Q}(\sqrt{d_i})$. By Theorem 1, the number of solutions of $x_i^2 - d_i y_i^2 = 1$ with $|x_i|, |y_i| < N$ is $\varrho_i \log N + O(1)$. Hence, for the decomposable form equation

$$\prod_{i=1}^t (x_i^2 - d_i y_i^2) = 1,$$

one cannot expect any better than $P(N) = \varrho(\log N)^t + O((\log N)^{t-1})$.

3. Counting units in abelian group rings. Let Γ denote a finite abelian group, with $\mathbb{Z}\Gamma$ denoting the integral group ring. This is the ring which consists of all expressions $\sum_{\gamma \in \Gamma} x_\gamma \gamma$ for $x_\gamma \in \mathbb{Z}$. Addition is linear and multiplication is taken with respect to the group operation in Γ. Let T_Γ denote the subgroup of $\mathbb{Z}\Gamma^*$ defined by $T_\Gamma = \{\pm\gamma : \gamma \in \Gamma\}$. It is known that

$\mathbb{Z}\Gamma^*$ is a finitely-generated group. Also, Higman's Theorem says that the torsion subgroup is precisely T_Γ. Let r_Γ denote the torsion-free rank. There is considerable interest in the group $\mathbb{Z}\Gamma^*$ (see [10], [12]). In [1], the distribution of the elements in this group was studied because of the relationship with the distribution of normal integral bases. Of particular interest is the distribution of these units with respect to the following Euclidean norm: define $|x| = |\sum_\gamma x_\gamma \gamma| = \max_\gamma\{|x_\gamma|\}$. Let $U_\Gamma(N)$ denote the counting function

$$U_\Gamma(N) = \#\{x \in \mathbb{Z}\Gamma^* : |x| < N\}.$$

From our theorems, the following arise as special cases.

THEOREM 3. *Let Γ denote a finite abelian group, with $r_\Gamma > 0$ denoting the torsion-free rank of $\mathbb{Z}\Gamma^*$. Then we have an asymptotic formula*

$$U_\Gamma(N) = \mu_\Gamma(\log N)^{r_\Gamma} + O((\log N)^{r_\Gamma - 1}) \quad \text{as } N \to \infty, \tag{3.1}$$

where $\mu_\Gamma > 0$. Suppose Γ does not have a cyclic factor group of order 5, 8, 10 *or* 12 *and $r_\Gamma > 1$. Then we have the following asymptotic formula*:

$$\begin{aligned} U_\Gamma(N) = \mu_\Gamma(\log N)^{r_\Gamma} &+ \nu_\Gamma(\log N)^{r_\Gamma - 1} \\ &+ o((\log N)^{r_\Gamma - 1}) \quad \text{as } N \to \infty. \end{aligned} \tag{3.2}$$

Proof. We will prove (3.1) and (3.2) simultaneously. For (3.1), it is sufficient to prove that the elements $x \in \mathbb{Z}\Gamma^*$ correspond to the integer solutions of a finite number of decomposable form equations, with coefficients in $\mathbb{Z}$. For (3.2), we need to check that the associated number fields satisfy the conditions of Theorem 2. Let $\widehat{\Gamma}$ denote the character group of Γ. Each $\chi \in \widehat{\Gamma}$ defines a linear form on $\mathbb{Z}\Gamma$ as follows: $\chi(x) = \sum_\gamma x_\gamma \chi(\gamma)$. In [1], it was proved that for $x \in \mathbb{Z}\Gamma$, we have $x \in \mathbb{Z}\Gamma^*$ if and only if

$$\prod_{\chi \in \widehat{\Gamma}} \chi(x) = \pm 1. \tag{3.3}$$

Thus, if n denotes the order of Γ then the elements $x \in \mathbb{Z}\Gamma^*$ can be identified with the integer solutions $\mathbf{x} \in \mathbb{Z}^n$ of two decomposable form equations (corresponding to the two choices of sign on the right in (3.3)). We need to prove that the coefficients lie in $\mathbb{Z}$. Let Ω denote the absolute Galois group, $\Omega = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then Ω acts on $\widehat{\Gamma}$ in the obvious way. Let $\mathfrak{C}$ denote the set of equivalence classes of $\widehat{\Gamma}$ under this action. For each class $c \in \mathfrak{C}$, let χ_c denote a representative character. Now the group Ω acts on the form on the left of (3.3). It permutes the characters in any particular class. Thus, every character appears as often as any of its Galois conjugates. This shows that Ω preserves the form. Since the coefficients are algebraic integers, it follows that they actually lie in $\mathbb{Z}$.

Let $\mathbb{Q}_c = \mathbb{Q}(\chi_c)$ denote the extension field generated by the values of χ_c. We can re-write the left of (3.3) as

$$\prod_{\chi\in\widehat{\Gamma}} \chi(x) = \prod_c N_{\mathbb{Q}_c|\mathbb{Q}}(\chi_c(x)),$$

where $\chi_c \in c$ is some fixed choice of character. Since Γ is abelian, its character values are roots of unity so each of the fields $\mathbb{Q}(\chi_c)$ is cyclotomic. In particular, these fields are totally real fields or totally imaginary quadratic extensions of totally real fields. The only cyclotomic fields which have unit rank equal to 1 are those of order 5, 8, 10 and 12. Since these extensions are generated by character values we must exclude characters which have orders 5, 8, 10 or 12. The character group $\widehat{\Gamma}$ is naturally isomorphic to Γ. By duality, subgroups of $\widehat{\Gamma}$ correspond to factor groups of Γ. This explains the restriction on the factor groups of Γ to allow (3.2).

We can go further and identify the underlying algebra as the group algebra $\mathbb{Q}\Gamma$. Note that the factors of the decomposable form are linearly independent. The matrix of coefficients is $L = (\chi(\gamma))$ where χ runs over $\widehat{\Gamma}$ and γ runs over Γ. The orthogonality relations for abelian characters imply the relation $L\overline{L}^t = nI_n$, where $\overline{L}^t$ denotes the conjugate transpose of L and I_n denotes the $n \times n$ identity matrix. Thus, L is certainly non-singular. Then the map

$$x \mapsto (\chi_c(x)), \qquad x \in \mathbb{Q}\Gamma, \tag{3.4}$$

is a ring homomorphism between the group algebra $\mathbb{Q}\Gamma$ and the algebra $\prod_c \mathbb{Q}_c$. The non-singularity of L guarantees this map is an isomorphism. Thus the map in (3.4) is an isomorphism between the underlying algebra of the form in (3.3) and the group algebra $\mathbb{Q}\Gamma$.

For an alternative description of this isomorphism, see Corollary 8.9.9 in [10]. On both sides of the isomorphism, the maximal order is the integral closure of $\mathbb{Z}$. Thus the map preserves maximal orders and it follows that the unit group $\mathbb{Z}\Gamma^*$ maps onto a subgroup of finite index of the product of the unit groups of the fields $\mathbb{Q}_c$. Thus, $\mathbb{Z}\Gamma^*$ has the same torsion free rank as this product group. This means there is a family of solutions corresponding to the whole group algebra $\mathbb{Q}\Gamma$. Thus we may take $r = r_\Gamma$ in Theorems 1 and 2. Finally, let $d_c = [\mathbb{Q}(\chi_c) : \mathbb{Q}]$; then we have $n = |\Gamma| = \sum_c d_c$ and this means that the condition on the subfields in the statement of Theorem 2 can be omitted. This completes the proof that Theorem 3 follows from Theorems 1 and 2. ■

Example. Let $\Gamma = C_7$, the cyclic group of order 7. There are two classes of characters and the algebra corresponding to the form is the group algebra

$$\mathbb{Q}\Gamma \simeq \mathbb{Q} \times \mathbb{Q}(\zeta_7). \tag{3.5}$$

In (3.5), ζ_7 denotes any primitive 7th root of unity. If $\Gamma = \langle\tau\rangle$, let $v = 1-\tau-\tau^6$, $w = 1-\tau^2-\tau^5$. Then $v, w \in \mathbb{Z}\Gamma^*$ ($v^{-1} = -1-\tau+\tau^3+\tau^4-\tau^6$, $w^{-1} = -1+\tau-\tau^2-\tau^5+\tau^6$) and it can be shown that $\mathbb{Z}\Gamma^* \simeq T_\Gamma \times \langle v, w\rangle$. Thus $r_\Gamma = 2$ and Theorem 2 applies, so in this special case we deduce that

$$U_\Gamma(N) = \mu_\Gamma(\log N)^2 + \nu_\Gamma \log N + o(\log N).$$

4. Proof of Theorem 1. The following lemma will play a basic role in the proofs of Theorems 1 and 2. It is a consequence of the main result of [7], whose proof depends upon Schlickewei's p-adic generalisation of the Subspace Theorem.

LEMMA 1. *The set of solutions of* (2.2) *is a union of finitely many families of solutions.*

Proof. In [7] and [5], the equation

$$cN_{A|\mathbb{Q}}(x) = \pm a, \qquad x \in \mathfrak{M}, \tag{2.2$'$}$$

was considered in a more general situation. With the notation of Section 2, $E_{\mathfrak{M},B} = \{\varepsilon \in O_B^* : \varepsilon\mathfrak{M}^B = \mathfrak{M}^B\}$ is a subgroup of finite index in O_B^* (cf. [7]). If $x \in \mathfrak{M}^B$ is a solution of (2.2′) then so is every element of $xE_{\mathfrak{M},B}$. Such a set $xE_{\mathfrak{M},B}$ is called an $(\mathfrak{M}, B)$-family of solutions of (2.2′). It follows from the main result in [7] (cf. also [5]) that the set of solutions of (2.2′) is the union, say $\bigcup_{j=1}^u x_jE_{\mathfrak{M},B_j}$ of families of solutions, where x_j is a solution of (2.2′) and B_j is a $\mathbb{Q}$-subalgebra of A with $1_A \in B_j$.

Denote by J the subset of $\{1,\ldots,u\}$ such that for each $j \in J$, $x_jE_{\mathfrak{M},B_j}$ contains at least one element which is a solution of (2.2). If $j \in J$, we may assume that x_j is a solution of (2.2). The group $U_{\mathfrak{M},B_j}$ defined in Section 2 is a subgroup of index 1 or 2 in $E_{\mathfrak{M},B_j}$. Thus it follows that the set of solutions of (2.2) can be expressed as $\bigcup_{j\in J} x_jU_{\mathfrak{M},B_j}$, which completes the proof. ■

Let $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n) \in \overline{\mathbb{Q}}^n - \{\mathbf{0}\}$. Let K denote any algebraic number field containing $\alpha_1,\ldots,\alpha_n$ and let $\tau_1,\ldots,\tau_d$ denote the isomorphic embeddings of K into $\overline{\mathbb{Q}}$, where $d = [K:\mathbb{Q}]$. Let $(\boldsymbol{\alpha})$ denote the fractional ideal of K generated by $\alpha_1,\ldots,\alpha_n$, with $N_{K|\mathbb{Q}}((\boldsymbol{\alpha}))$ denoting its norm. The *absolute* (*multiplicative*) *Weil height* of $\boldsymbol{\alpha}$ is defined to be

$$\overline{H}(\boldsymbol{\alpha}) = \overline{H}(\alpha_1,\ldots,\alpha_n) = \left\{\frac{\prod_{i=1}^d \max\{|\tau_i(\alpha_1)|,\ldots,|\tau_i(\alpha_n)|\}}{N_{K|\mathbb{Q}}((\boldsymbol{\alpha}))}\right\}^{1/d}. \tag{4.1}$$

Obviously, $\overline{H}(\boldsymbol{\alpha})$ does not depend upon the choice of K. Further,

$$\overline{H}(\lambda\boldsymbol{\alpha}) = \overline{H}(\boldsymbol{\alpha}) \quad \text{for } \boldsymbol{\alpha} \in \overline{\mathbb{Q}}^n - \{\mathbf{0}\},\ \lambda \in \overline{\mathbb{Q}}^*.$$

As before, let A denote the algebra $M_1 \oplus \ldots \oplus M_t$. We define the *height* of $\xi = (\xi_1,\ldots,\xi_t) \in A$ to be the absolute Weil height of the vector with components consisting of $\xi_1,\ldots,\xi_t$ and their conjugates over $\mathbb{Q}$. Thus, if $\sigma_{i,1},\ldots,\sigma_{i,n_i}$ denote the embeddings of M_i into $\overline{\mathbb{Q}}$, $i=1,\ldots,n_i=[M_i:\mathbb{Q}]$, then

$$\overline{H}(\xi)=\overline{H}(\sigma_{1,1}(\xi_1),\ldots,\sigma_{1,n_1}(\xi_1),\ldots,\sigma_{t,1}(\xi_t),\ldots,\sigma_{t,n_t}(\xi_t)).$$

For every $H>0$, denote by $N(H)$ the number of solutions x of (2.2) with $\overline{H}(x)<H$. For a $\mathbb{Q}$-subalgebra B of A with $1_A\in B$, let r_B be defined as in Section 2.

LEMMA 2. *Suppose that* (2.2) *has infinitely many solutions. There is an asymptotic formula*

$$N(H)=\varrho(\log H)^r+O((\log H)^{r-1})\qquad \textit{as } H\to\infty,$$

where ϱ is a positive number independent of H and $r>0$ denotes the maximum of the r_B taken over all $\mathbb{Q}$-subalgebras B of A with $1_A\in B$ for which equation (2.2) *has an $(\mathfrak{M},B)$-family of solutions.*

Proof. A similar result was proved in [5] for equation (2.2′) above under the assumption that x and $-x$ are identified. Our Lemma 2 can be proved in the same way. In the proof of Corollary 4 of [5] it is enough to use our Lemma 1 instead of Theorem 1 of [5] and to choose $K=\mathbb{Q}$ with S denoting the ordinary absolute value, the trivial group $\{1\}$ instead of O_S^* and the families of solutions of (2.2) instead of those of (2.2′). ∎

In our paper, it will be more convenient to work with a slightly different height $H(\xi)$ for elements ξ of A. With the above notation, for $\xi=(\xi_1,\ldots,\xi_t)\in A$, we define

$$H(\xi)=\max_{i,j}\{|\sigma_{i,j}(\xi_i)|\}.$$

Proof of Theorem 1. Let K denote the splitting field of the decomposable form F over $\mathbb{Q}$, and let $d=[K:\mathbb{Q}]$. Consider equation (1.5) in the form (2.2). Let $g=\sum_{i=1}^t n_i$. There is a positive rational integer λ, depending only upon F and a, such that for each solution $\mathbf{x}$ of (1.5), (2.2) is equivalent to

$$c'N_{A|\mathbb{Q}}(x')=a',\qquad x'\in\mathfrak{M},\tag{4.2}$$

where $c'=\lambda c$ and $a'=\lambda^{g+1}a$ are already rational integers and $x'=\lambda x\in O_A$. Thus setting $x'=(\xi_1',\ldots,\xi_t')$, we have by (4.1),

$$H(x')=\overline{H}(x')N_{K|\mathbb{Q}}((\sigma_{1,1}(\xi_1'),\ldots,\sigma_{t,n_t}(\xi_t')))^{1/d}.$$

But $N_{K|\mathbb{Q}}((\sigma_{1,1}(\xi_1'),\ldots,\sigma_{t,n_t}(\xi_t')))$ is a positive integer which divides $N_{K|\mathbb{Q}}(\xi_i')$ in $\mathbb{Z}$, for each i. In view of (2.1) and (4.2), it follows that this latter norm is bounded above by a number which is independent of x'. Since $\overline{H}(x')=\overline{H}(x)$ and $H(x')=\lambda H(x)$, we deduce

$$c_1\overline{H}(x)\le H(x)\le c_2\overline{H}(x),\tag{4.3}$$

for each solution x of (2.2), where c_1, c_2 are positive constants. Since, by assumption, F has n linearly independent linear factors over $\overline{\mathbb{Q}}$, the map $\mathbf{x} \mapsto x = (L_i(\mathbf{x}))_{1\le i\le t}$ establishes a one-to-one correspondence between the solutions $\mathbf{x}$ of (1.5) and the solutions x of (2.2). Taking the conjugates of the linear factors L_i, $i = 1, \ldots, t$, and using Cramer's Rule, we deduce that for the corresponding solutions $\mathbf{x}$ of (1.5) and x of (2.2), we have

$$c_3 H(x) \le |\mathbf{x}| \le c_4 H(x). \tag{4.4}$$

In (4.4), c_3 and c_4 denote positive constants. Then by (4.3) and (4.4), to each solution $\mathbf{x}$ of (1.5) with $|\mathbf{x}| < N$, there corresponds a solution x of (2.2) with $\overline{H}(x) \le c_5 N$ for some $c_5 > 0$. By Lemma 2, we have

$$\begin{aligned} P(N) &\le \varrho(\log N + \log c_5)^r + O((\log N + \log c_5)^{r-1}) \\ &= \varrho(\log N)^r + O((\log N)^{r-1}). \end{aligned} \tag{4.5}$$

Conversely, there is a constant $c_6 > 0$ such that to each solution x of (2.2) with $\overline{H}(x) \le c_6 N$ there corresponds a solution $\mathbf{x}$ of (1.5) with $|\mathbf{x}| < N$. Hence, by Lemma 2 again, we deduce

$$\begin{aligned} P(N) &\ge \varrho(\log N + \log c_6)^r + O((\log N + \log c_6)^{r-1}) \\ &= \varrho(\log N)^r + O((\log N)^{r-1}). \end{aligned} \tag{4.6}$$

Now (4.5) and (4.6) imply (1.2). ■

5. Proof of Theorem 2. We use the notation of Sections 1–4. In particular, the one-to-one correspondence $\mathbf{x} \mapsto x = (L_1(\mathbf{x}), \ldots, L_t(\mathbf{x}))$ between the solutions of (1.5) and (2.2). Let B denote a $\mathbb{Q}$-subalgebra of A with $1_A \in B$. As was shown in [5], there is a partition $P = \{P_1, \ldots, P_q\}$ of $\{1, \ldots, t\}$, depending only upon B, and there are algebraic number fields $K_1, \ldots, K_q$ which are uniquely determined by B, with the following property: let $1_{P_s} = (\xi_1, \ldots, \xi_t) \in A$ with $\xi_i = 1$ if $i \in P_s$ and $\xi_i = 0$ otherwise then

$$B = \Big\{ \sum_{s=1}^{q} 1_{P_s} \eta_s : \eta_s \in K_s,\ s = 1, \ldots, q \Big\}. \tag{5.1}$$

Further, K_s is a subfield of M_i for $i \in P_s$. This implies that

$$O_B^* \simeq O_{K_1}^* \times \ldots \times O_{K_q}^*, \tag{5.2}$$

where $O_{K_s}^*$ denotes the unit group of the ring of integers of K_s, $s = 1, \ldots, q$.

Let $\mathfrak{F}_B$ denote an $(\mathfrak{M}, B)$-family of solutions of (2.2). We recall that r_B denotes the rank of O_B^*. Let $P_{\mathfrak{F}_B}(N)$ denote the number of solutions of (1.5) with $|\mathbf{x}| < N$ and with $\mathbf{x}$ corresponding to elements of the family $\mathfrak{F}_B$.

Lemma 3. *If $r_B > 1$ then there are real numbers $\varrho_{\mathfrak{F}_B} > 0$ and $\delta_{\mathfrak{F}_B}$ such that*

$$P_{\mathfrak{F}_B}(N) = \varrho_{\mathfrak{F}_B}(\log N)^{r_B} + \delta_{\mathfrak{F}_B}(\log N)^{r_B-1} + o((\log N)^{r_B-1}) \quad \textit{as } N \to \infty.$$

Firstly we deduce Theorem 2 from Lemmas 1 and 3. Lemma 3 will be proved later.

Proof of Theorem 2. By Lemma 1, the set of solutions of (2.2) is a union

$$\mathfrak{F}_1 \cup \ldots \cup \mathfrak{F}_u, \tag{5.3}$$

where for each j, $\mathfrak{F}_j$ is an $(\mathfrak{M}, B_j)$-family of solutions of (2.2), for some $\mathbb{Q}$-subalgebra B_j of A with $1_A \in B_j$. We may assume that for at least one of the j, r_{B_j} is maximal, i.e. $r_{B_j} = r$. We may also suppose that we deal with the case where $r_{B_j} \ge 1$. We show that $r_{B_j} \ge 1$ implies $r_{B_j} > 1$. Each $B = B_j$ can be written in the form (5.1). This gives $r_B = \sum_{s=1}^{q} \operatorname{rank} O_{K_s}^*$. It follows from our assumptions about the subfields of M_i that $\operatorname{rank} O_{K_s}^* \ge 2$ for at least one s, whence $r_B \ge 2$, proving our claim.

For a tuple $J = \{j_1, \ldots, j_v\}$ of integers from $\{1, \ldots, u\}$ with $j_1 < \ldots < j_v$, let $B_J = B_{j_1} \cap \ldots \cap B_{j_v}$, $\mathfrak{F}_J = \mathfrak{F}_{j_1} \cap \ldots \cap \mathfrak{F}_{j_v}$ and let $P_J(N)$ denote the number of solutions $\mathbf{x}$ of (1.5) with $\mathbf{x}$ corresponding to elements of $\mathfrak{F}_J$. It follows from Lemma 3 of [5] that $\mathfrak{F}_J$ is the union of finitely many $(\mathfrak{M}, B_J)$-families. By Lemma 3,

$$P_J(N) = \varrho_J(\log N)^r + \delta_J(\log N)^{r-1} + o((\log N)^{r-1}) \quad \text{as } N \to \infty, \tag{5.4}$$

where $\varrho_J > 0$ if $r_{B_J} = r$, $\varrho_J = 0$ if $r_{B_J} < r$ and $\delta_J = 0$ if $r_{B_J} < r - 1$. Now by the inclusion-exclusion principle, it follows from (5.3) that

$$P(N) = \sum_{j=1}^{u} P_j(N) - \sum_{|J|=2} P_J(N) + \sum_{|J|=3} P_J(N) - \ldots,$$

where

$$\varrho = \sum_{j=1}^{u} \varrho_j - \sum_{|J|=2} \varrho_J + \sum_{|J|=3} \varrho_J - \ldots$$

We have $P(N) \ge P_j(N)$ for $j = 1, \ldots, u$, hence $\varrho \ge \varrho_j$ for $j = 1, \ldots, u$. But for some j we have $\varrho_j > 0$ thus $\varrho > 0$. This proves the asymptotic formula desired for $P(N)$.

If, in particular, $n = \deg F = \sum_{i=1}^{t} [M_i : \mathbb{Q}]$ then in (2.2), $\mathfrak{M}$ generates A over $\mathbb{Q}$. In this case, the set of solutions of (2.2) is the union of finitely many pairwise distinct $(\mathfrak{M}, A)$-families of solutions (cf. [7]). Now the assertion of Theorem 2 follows as above without any assumption on the unit ranks of the subfields of $M_1, \ldots, M_t$. This completes the proof of Theorem 2. ∎

Now we go on to prove Lemma 3. Let $\mathfrak{F}_B$ denote an $(\mathfrak{M}, B)$-family of solutions with $r_B > 0$. Then $\mathfrak{F}_B = x'U_{\mathfrak{M},B}$, where x' is a solution of (2.2) with $x' \in \mathfrak{M}^B$. Consider the subgroup of O_B^* consisting of elements $(\xi_1, \ldots, \xi_t)$ with real components. We note that by the assumption made on the fields M_i in Theorem 2, all the components here are totally real. Let U_B denote the intersection of the maximal torsion-free subgroup of this latter subgroup with $U_{\mathfrak{M},B}$.

LEMMA 4. *U_B is a subgroup of finite index both in $U_{\mathfrak{M},B}$ and in O_B^*. Further, there are finitely many elements $x_1, \ldots, x_w$ in $\mathfrak{F}_B$ such that the x_iU_B form a partition of $\mathfrak{F}_B$ into pairwise disjoint subsets.*

Proof. By assumption, each number field $M_i, i = 1, \ldots, t$, is either a totally real field or a totally imaginary quadratic extension of a totally real field. As is known (see e.g. [6]), each subfield of M_i is also of this type. In particular, this applies to the fields K_s, $s = 1, \ldots, q$, in the representation (5.1). Further, for each s, the maximal torsion-free subgroup of the group of real units in K_s is of finite index in $O_{K_s}^*$ (see also [6]). In view of (5.2), this implies that the maximal torsion-free subgroup of O_B^* consisting of elements with real components in A is also of finite index in O_B^*. Since $U_{\mathfrak{M},B}$ is also of finite index in O_B^* (see [7]), it follows that U_B is of finite index both in $U_{\mathfrak{M},B}$ and in O_B^*. If $y_1, \ldots, y_w$ is a full set of representatives for the cosets of U_B in $U_{\mathfrak{M},B}$ then the assertion follows with the choice $x_i = x'y_i$ for $i = 1, \ldots, w$. ∎

Let B and $U = U_B$ carry the same meaning as in Lemma 4. Let x_0 be a solution of (2.2) with $x_0 \in \mathfrak{M}^B$ and let $P_{x_0,U}(N)$ denote the number of solutions of (1.5) with $|\mathbf{x}| < N$ and with $\mathbf{x}$ corresponding to the set of solutions x_0U.

PROPOSITION. *Under the assumptions above, let $r_B > 1$. Then*

$$P_{x_0,U}(N) = \varrho_{x_0,U}(\log N)^{r_B} + \delta_{x_0,U}(\log N)^{r_B-1} + o((\log N)^{r_B-1})$$

as $N \to \infty$, where $\varrho_{x_0,U} > 0$ and $\delta_{x_0,U}$ are real numbers.

Proof of Lemma 3. This is immediate from the Proposition and Lemma 4. ∎

It remains to prove the Proposition and this requires some more lemmas. To simplify notation, we assume B is chosen with $r = r_B$. For those B with $r_B < r$, we can proceed in the same way. We will assume that B and O_B^* are represented as in (5.1) and (5.2). For non-zero elements $\alpha \in A$, we use the notation $h(\alpha) = \log H(\alpha)$.

We will pass to logarithmic space where we apply the geometry of numbers. Our results can now be described by modelling the whole set-up in the following general way. It is sufficient to count the logarithms of the absolute values of the conjugates of the component units below a fixed bound. But these are linear forms which arise in the following way. By Lemma 4, U is free of rank r, hence each element of U can be expressed in terms of basis elements, say $f_1, \dots, f_r$. Then (with componentwise multiplication), each $u \in U$ may be expressed as

$$u = f_1^{e_1} \dots f_r^{e_r}, \qquad \mathbf{e} = (e_1, \dots, e_r) \in \mathbb{Z}^r.$$

Thus each component u_i of u looks like $f_{i1}^{e_1} \dots f_{ir}^{e_r}$ for some algebraic numbers $f_{ij}, j = 1, \dots, r$. By (5.1) and (5.2), it is easy to see that for fixed i, these f_{ij} generate a subgroup of finite index in the unit group of the subfield K_s of M_i. The logarithm of the absolute value of any conjugate of u_i is a linear form in $\mathbf{e}$ with real coefficients. Thus we have a collection of real linear forms $\phi_l(\mathbf{e})$, $l = 1, \dots, d$, $\mathbf{e} \in \mathbb{R}^r$, where $d = \sum_s d_s$ and $d_s = [K_s : \mathbb{Q}]$, which correspond to the logarithms of the absolute values of the conjugates of the units, which are the components of u in A. These forms have rank r and $\sum_l \phi_l = 0$ identically by the unit condition. Each of these forms which is not identically zero has at least two coefficients which are linearly independent over $\mathbb{Q}$. This follows from our assumption about the unit ranks of the subfields of the fields M_i. In what follows, only those forms ϕ_l which are not identically zero will be considered. For any vector $\mathbf{e} \in \mathbb{R}^r$, define

$$\phi(\mathbf{e}) = \max_l \{\phi_l(\mathbf{e})\}. \tag{5.5}$$

The forms $\phi_l(\mathbf{e})$ have rank r. This, together with the condition $\sum_l \phi_l(\mathbf{e}) = 0$, $\mathbf{e} \in \mathbb{R}^r$, guarantees that $\phi(\mathbf{e})$ is commensurate with $|\mathbf{e}|$. This fact was pointed out in Lemma 2.2 of [4]. Geometrically, the region $\phi(\mathbf{e}) < Y$ for real $Y > 0$ defines a polytope. Thus the number of lattice points within that region is easily estimated by the volume of the region, with an error term of order equal to the volume of the boundary. In fact, much more can be (and has been) said. The following formula arises as a direct application of Proposition 2.1 in [4]:

$$\phi(Y) = \#\{\mathbf{x} \in \mathbb{Z}^r : \phi(\mathbf{e}) < Y\} = C_1 Y^r + o(Y^{r-1}). \tag{5.6}$$

In (5.6), C_1 denotes a positive constant. Let

$$U(X) = \#\{u \in U : H(u) < X\}.$$

We will also require an estimate of the number of elements of U with a particular conjugate as largest. Given $s = 1, \dots, q$, let $\tau_{sj} : K_s \to \overline{\mathbb{Q}}$ denote an embedding. Define U_{sj} by

$$U_{sj} = \{u \in U : H(u) = |\tau_{sj}(u_s)|\}.$$

Let $U_{sj}(X)$ denote the corresponding counting function

$$U_{sj}(X) = \#\{u \in U_{sj} : H(u) < X\}.$$

LEMMA 5. *We have*

$$U(X) = C_1(\log X)^r + o((\log X)^{r-1}), \tag{5.7}$$

$$U_{sj}(X) = C_2(s,j)(\log X)^r + C_3(s,j)(\log X)^{r-1} + o((\log X)^{r-1}). \tag{5.8}$$

Proof. Of course (5.7) is a re-statement of (5.6) with $Y = \log X$. To prove (5.8) we appeal to Lemma 3.2 in [4] (with $p_s = 0, q_s = 1$ and $N = 1$). ■

In order to prove our Proposition, we will need the following refinement of Lemma 5. Let $H^*(u)$ (respectively $H^{**}(u)$) denote the second (respectively third) largest element of the set $\{|\tau_{sj}(u_s)|\}_{s,j}$. This set is composed of all the absolute values of all the conjugates of the components in u and we do allow repetitions; thus $H(u) = H^*(u)$ is allowable, for example. Let $C_4 > 1$ and $C_5 > 1$ denote constants. Define the following sets:

$$U^* = \{u \in U : H^*(u)/H(u) < C_4/h(u)^{C_5}\},$$
$$U^{**} = \{u \in U : H^{**}(u)/H(u) < C_4/h(u)^{C_5}\}.$$

In what follows, we are generally unconcerned about the precise values of C_4 and C_5 since our formulae do not depend upon these values in any important way (see Lemma 6 for example). This explains why the notation is chosen also to be independent of any mention of them. Define the basic counting function of U^{**} as follows:

$$U^{**}(X) = \#\{u \in U^{**} : H(u) < X\}.$$

Also, let

$$U_{sj}^* = U_{sj} \cap U^*, \quad U_{sj}^{**} = U_{sj} \cap U^{**},$$
$$U_{sj}^{**}(X) = \#\{u \in U_{sj}^{**} : H(u) < X\}.$$

LEMMA 6. *There are asymptotic formulae as follows*:

$$U^{**}(X) = C_1(\log X)^r + o((\log X)^{r-1}), \tag{5.9}$$

$$U_{sj}^{**}(X) = C_2(s,j)(\log X)^r + C_3(s,j)(\log X)^{r-1} + o((\log X)^{r-1}), \tag{5.10}$$

where C_1, C_2, C_3 denote the same constants as in Lemma 5.

Proof. For any $\mathbf{e} \in \mathbb{R}^r$, let $\phi^*(\mathbf{e})$ (respectively $\phi^{**}(\mathbf{e})$) denote the second (respectively third) largest element of the set $\{\phi_l(\mathbf{e})\}$ in (5.5). Suppose $C_6 = \log C_4$ and define

$$\phi^{**} = \{\mathbf{0} \neq \mathbf{e} \in \mathbb{R}^r : \phi^{**}(\mathbf{e}) - \phi(\mathbf{e}) < C_6 - C_5 \log \phi(\mathbf{e})\}$$

and

$$\phi^{**}(Y) = \#\{\mathbf{e} \in \mathbb{Z}^r \cap \phi^{**} : \phi(\mathbf{e}) < Y\}.$$

Clearly, the formula in (5.9) is equivalent to the following statement:

$$\phi^{**}(Y) = C_1 Y^r + o(Y^{r-1}). \tag{5.11}$$

Proof of (5.11). It is sufficient to estimate the size of the complementary set

$$\{\mathbf{e} \in \mathbb{Z}^r : \phi(\mathbf{e}) < Y,\ \phi(\mathbf{e}) \le \phi^{**}(\mathbf{e}) + C_5 \log \phi(\mathbf{e}) - C_6\},$$

in the set considered in (5.6) and show this estimate lies in the error term. Now $\phi^{**}(\mathbf{e}) \le \phi(\mathbf{e})$ always so the complementary set is contained within the set

$$\{\mathbf{e} \in \mathbb{R}^r : \phi(\mathbf{e}) < Y,\ |\phi(\mathbf{e}) - \phi^{**}(\mathbf{e})| < C_5 \log \phi(\mathbf{e})\}.$$

However since $\phi(\mathbf{e}) < Y$, we see that this set is contained in

$$\{\mathbf{e} \in \mathbb{R}^r : \phi(\mathbf{e}) < Y,\ |\phi(\mathbf{e}) - \phi^{**}(\mathbf{e})| < C_5 \log Y\}. \tag{5.12}$$

The set in (5.12) is a measurable region since its boundary is defined by piecewise linear maps. Thus the number of lattice points the region contains can be estimated by the sum of the (r-dimensional) measure of the region and the ($r-1$-dimensional) measure of the boundary of the region. Geometrically, the claims we make about this, and similar, regions are fairly obvious since the basic object of study is a polytope in a real, r-dimensional space. For a formal proof, place a unit cube around each of the lattice points. Count 1 towards the volume of the region every time the cube is interior to the region. If the cube intersects the boundary of the region, count 1 towards the volume of the boundary. Both of these measures are easily estimated by integrating via substitution. Let θ_1 denote the largest of the $\phi_l(\mathbf{e})$, with θ_2 denoting the second largest and so on up to θ_r. There are only finitely many possible orderings of the θ_i. It follows that the Jacobian of this transformation is piecewise constant and thus it is certainly bounded. With our new variables, we inherit the inequality $|\theta_1 - \theta_3| < C_5 \log Y$. Each of the new variables is bounded above by Y and we need to place some lower bound also. Since $\sum_l \phi_l(\mathbf{e}) = 0$ identically and $\phi(\mathbf{e}) < Y$, we see that each $\phi_l(\mathbf{e}) > -(d-1)Y$. Thus we impose this same lower bound on each of the $\theta_i, i = 1, \ldots, r$. (Since $\theta_1 \ge 0$ always, this is quite a concession.) Then compute the measure of the set

$$\{\boldsymbol{\theta} \in \mathbb{R}^r : -(d-1)Y \le \theta_r \le \ldots \le \theta_1 < Y,\ |\theta_1 - \theta_3| < C_5 \log Y\}. \tag{5.13}$$

The total contribution to the integral from the θ_1 and θ_2 variables is $O((\log Y)^2)$. Integrating over the remaining $r-2$ variables gives a contribution of $O(Y^{r-2})$. Multiplying these two gives a term $O(Y^{r-2}(\log Y)^2)$ which is within the error term required by (5.11). On the boundary, one of the inequalities in (5.13) must be changed to an equality with the corresponding variables being identified. A similar argument now gives the same error term.

Proof of (5.10). Using the ϕ-notation, those elements in the complementary set are already contained within the set in (5.13). This is because they correspond to a particular choice of forms as first and second largest. Since we showed that the number of lattice points in (5.13) is already counted in the error term, it follows that the number of lattice points in a subset will be so counted. ■

We are counting solutions $\mathbf{x} \in \mathbb{Z}^n$ of (1.5) corresponding to the set of solutions $x_0 U$ considered above. By (1.4), (1.5), (2.1) and (2.2), there are constants b_i and units u_i such that

$$L_i(\mathbf{x}) = b_i u_i, \tag{5.14}$$

where $x_0 = (b_1, \ldots, b_t)$ and $u = (u_1, \ldots, u_t) \in U$. For each $i = 1, \ldots, t$, there are $n_i = [M_i : \mathbb{Q}]$ conjugate embeddings $\sigma_{ij} : M_i \to \overline{\mathbb{Q}}$ and the image of each u_i under σ_{ij} lies in $\mathbb{R}$. Applying these to the equations in (5.14), we obtain $\sum_{i=1}^{t} n_i$ linear equations which we write as

$$L_{ij}(\mathbf{x}) = b_{ij} u_{ij}, \quad \mathbf{x} = (x_1, \ldots, x_n),\ i = 1, \ldots, t,\ j = 1, \ldots, n_i. \tag{5.15}$$

We are assuming that among the L_{ij}, there are n linearly independent linear forms. We will use that fact to express the entries x_i in $\mathbf{x}$ as linear combinations of the u_{ij}. Choose a set of n linearly independent forms with the proviso that whichever $|u_{ij}|$ is largest, its corresponding form L_{ij} is in the set. This could be guaranteed by choosing that form first and then completing to an independent set. After re-labelling, we have a set of n equations,

$$L_l(\mathbf{x}) = b_l u_l, \quad l = 1, \ldots, n. \tag{5.16}$$

Using this representation, we are able to prove the following:

LEMMA 7. *Let* $\mathbf{x}$ *denote a solution of* $F(\mathbf{x}) = a$ (see (1.5)), *corresponding to* $x_0 u \in x_0 U$. *Then*:

(i) *We have*

$$\log |\mathbf{x}| = h(u) + O(1). \tag{5.17}$$

(ii) *For all* $s = 1, \ldots, q$ *and* $j = 1, \ldots, d_s = [K_s : \mathbb{Q}]$ *for which* U_{sj}^* *is infinite*, *there are constants* α_{sj} *such that for all* $u \in U_{sj}^*$,

$$\log |\mathbf{x}| = h(u) + \alpha_{sj} + O\left(\frac{1}{h(u)^{C_5}}\right). \tag{5.18}$$

Proof. (i) (This is similar to (4.4).) Clearly $H(u) < C_7 |\mathbf{x}|$ by (5.16) and the triangle inequality. Inverting the system of equations in (5.16) now gives a similar inequality in reverse. Taking logarithms gives (5.17).

(ii) Let $u \in U_{sj}^*$. It is sufficient to deal with the case where $h(u)$ is large enough. Then we have for each x_k,

$$x_k = \Omega_{sjk} \tau_{sj}(u_s) + O(H^*(u)) = \Omega_{sjk} \tau_{sj}(u_s) + O\left(\frac{H(u)}{h(u)^{C_5}}\right).$$

Assume that $|\mathbf{x}| = |x_{k_0}|$. Then Ω_{sjk_0} is not zero (otherwise we contradict (i)). We may write

$$x_{k_0} = \Omega_{sjk_0}\tau_{sj}(u_s)\left(1 + O\left(\frac{1}{h(u)^{C_5}}\right)\right). \tag{5.19}$$

Take the logarithm of the absolute value of both sides in (5.19). Using the estimate $\log(1+\varepsilon) = \varepsilon + O(\varepsilon^2)$ for small $\varepsilon > 0$ now gives

$$\log|\mathbf{x}| = h(u) + \log|\Omega_{sjk_0}| + O\left(\frac{1}{h(u)^{C_5}}\right). \tag{5.20}$$

Next assume k is chosen with $|\Omega_{sjk}|$ largest. Then we get, in the same way,

$$\log|x_k| = h(u) + \log|\Omega_{sjk}| + O\left(\frac{1}{h(u)^{C_5}}\right). \tag{5.21}$$

It follows from (5.20) and (5.21) that $|\Omega_{sjk_0}| = |\Omega_{sjk}|$. This proves (5.18) with the choice $\alpha_{sj} = \log|\Omega_{sjk}|$. ■

Proof of the Proposition. Recall that $P_{x_0,U}(N)$ denotes the number of solutions $\mathbf{x} \in \mathbb{Z}^n$ of (1.5) with $|\mathbf{x}| < N$ which correspond to x_0U. In other words, $P_{x_0,U}(N)$ is the number of $u \in U$ for which x_0u corresponds to a solution $\mathbf{x} \in \mathbb{Z}^n$ of (1.5) with $|\mathbf{x}| < N$. We decompose the counting function $P_{x_0,U}(N)$ according to the sets mentioned in our lemmas. Thus, a first decomposition arises as follows:

$$P_{x_0,U}(N) = \#\{u \in U^{**} : |\mathbf{x}| < N\} + \#\{u \in U - U^{**} : |\mathbf{x}| < N\}. \tag{5.22}$$

Using (5.7) in tandem with (5.9), we note that

$$\#\{u \in U - U^{**} : H(u) < N\} = o((\log N)^{r-1}). \tag{5.23}$$

By (5.17), there is a $C_8 > 0$ such that

$$\#\{u \in U - U^{**} : |\mathbf{x}| < N\} \le \#\{u \in U - U^{**} : h(u) < \log N + C_8\}$$

and by (5.23), the right hand side is $o((\log N)^{r-1})$.

For the first term on the right in (5.22), we make a further refinement as follows:

$$\sum_{s,j} \#\{u \in U^*_{sj} : |\mathbf{x}| < N\} + \sum_{s,j} \#\{u \in U^{**}_{sj} - U^*_{sj} : |\mathbf{x}| < N\}. \tag{5.24}$$

For the first term in (5.24), we invoke (5.18) which allows us to replace $\log|\mathbf{x}|$ essentially by $h(u) + \alpha_{sj}$. Thus (5.24) becomes

$$\sum_{s,j} \#\{u \in U^*_{sj} : h(u) < \log N - \alpha_{sj}\} \\ + \sum_{s,j} \#\{u \in U^{**}_{sj} - U^*_{sj} : |\mathbf{x}| < N\}. \tag{5.25}$$

Expand the first term of (5.25) by counting in U_{sj}^{**}:

$$\begin{aligned}(5.26)\qquad \sum_{s,j} \#\{u \in U_{sj}^{**} : h(u) < \log N - \alpha_{sj}\}& \\ - \sum_{s,j} \#\{u \in U_{sj}^{**} - U_{sj}^{*} : h(u) < \log N - \alpha_{sj}\}& \\ + \sum_{s,j} \#\{u \in U_{sj}^{**} - U_{sj}^{*} : |\mathbf{x}| < N\}.&\end{aligned}$$

The first term in (5.26) is $U_{sj}^{**}(N/e^{\alpha_{sj}})$ and the formula for this can be written down by applying (5.10):

$$(5.27)\quad \sum_{s,j} \{C_2(s,j)(\log N - \alpha_{sj})^r + C_3(s,j)(\log N)^{r-1} + o((\log N)^{r-1})\}.$$

By Lemma 5, $\sum_{s,j} C_2(s,j) = C_1$, which is positive. Hence formula (5.27) is clearly of the shape required by the Proposition. The proof of the Proposition will be finished by showing that the last two terms in (5.26) contribute only to the error term. Firstly, absorb them into one by reversing the inequality in the first bracket and by invoking (5.17) which allows us to replace $\log |\mathbf{x}|$ by $h(u) + O(1)$:

$$\sum_{s,j} \#\{u \in U_{sj}^{**} - U_{sj}^{*} : \log N - \alpha_{sj} \le h(u) < \log N + O(1)\}.$$

Then it is sufficient to estimate

$$(5.28)\qquad \#\{u \in U^{**} - U^{*} : |h(u) - \log N| < C_9\}.$$

In fact, we can estimate (5.28) by $O((\log N)^{r-2} \log\log N)$, which lies well within the error term. The heuristic is that the condition $u \in U^{**} - U^{*}$ and the inequality both surrender one degree of freedom. Using the notation of the proof of Lemma 6, we are counting lattice points in a region defined by inequalities

$$\begin{aligned}(5.29)\qquad \{\mathbf{e} \in \mathbb{R}^r : \phi(\mathbf{e}) < Y,\ |\phi(\mathbf{e}) - Y| < C_9,& \\ \phi^*(\mathbf{e}) \le \phi(\mathbf{e}) < \phi^*(\mathbf{e}) + C_{10} \log Y\},&\end{aligned}$$

where $Y = \log N$. The boundary of the region in (5.29) is defined by linear forms. Just as before, we may estimate the number of lattice points in the region by the sum of the volume of the region and the volume of the boundary. Change the variables by substituting θ_i for the ith largest of the $\phi_l(\mathbf{e})$, where $i = 1, \dots, r$. We apply the same lower bound as before for the new variables. It comes down to estimating the measure of a region

$$\begin{aligned}\{\boldsymbol{\theta} \in \mathbb{R}^r : -(d-1)Y \le \theta_r \le \dots \le \theta_1 < Y,\ |\theta_1 - Y| < C_9,& \\ \theta_2 \le \theta_1 \le \theta_2 + C_{10} \log Y\}.&\end{aligned}$$

Since θ_1 is constrained within an interval of bounded length, the total contribution from the θ_1 integral is obviously $O(1)$. Since θ_1 and θ_2 are at most $C_{10} \log Y$ apart, the contribution from the θ_2 integral is $O(\log Y)$. The contribution from the remaining variables is $O(Y^{r-2})$. Multiplying these error estimates gives a term which is $O(Y^{r-2} \log Y)$. Since $Y = \log N$ we obtain an error term well within that required by the Proposition. For the boundary, a similar argument gives the same error term. ■

Remark. From our analysis, it is clear that each of the coefficients x_i comprising $\mathbf{x}$ consist of a linear combination of $H(u)$ and $H^*(u)$ with an error term which is $O(H^{**}(u))$. To project the vector $\mathbf{x}$ centrally means to divide by the norm. Since any two norms are commensurate, altering the norm only affects the shape of the unit ball. It follows from (5.17) that $H(u)$ is commensurate with any norm so we may divide $\mathbf{x}$ by $H(u)$ to get an idea of the location of any cluster points. We see that the image on the unit ball is a vector $\mathbf{a}$ with an error term which is $O(H^*(u)/H(u))$. For "most" of the units, this error is vanishingly small and it follows that the vectors $\mathbf{a}$ form a finite collection of cluster points. We actually proved more in this paper, namely, units tend to have two dominant conjugates. This makes a statement about the lines on the ball which join the cluster points. In our next paper, we will examine more closely the coordinates of these points, and the lines which join them. This will involve a more detailed study of the distribution of the various x_k and not just $|\mathbf{x}|$.

References

[1] G. R. Everest, *Diophantine approximation and the distribution of normal integral generators*, J. London Math. Soc. 28 (1983), 227–237.

[2] —, *A 'Hardy–Littlewood' approach to the norm form equation*, Math. Proc. Cambridge Philos. Soc. 104 (1988), 421–427.

[3] —, *On the solution of the norm-form equation*, Amer. J. Math. 114 (1992), 667–681.

[4] —, *Mean values of algebraic linear forms*, Proc. London Math. Soc. 70 (1995), 529–555.

[5] J.-H. Evertse and K. Győry, *The number of families of solutions of decomposable form equations*, Acta Arith., to appear.

[6] K. Győry, *Sur une classe des corps de nombres algébriques et ses applications*, Publ. Math. Debrecen 22 (1975), 151–175.

[7] —, *On the numbers of families of solutions of systems of decomposable form equations*, ibid. 42 (1993), 65–101.

[8] K. Győry und A. Pethő, *Über die Verteilung der Lösungen von Normformen Gleichungen II*, Acta Arith. 32 (1977), 349–363.

[9] —, *Über die Verteilung der Lösungen von Normformen Gleichungen III*, ibid. 37 (1980), 143–165.

[10] G. Karpilovsky, *Unit Groups of Classical Rings*, Oxford University Press, 1988.

[11] W. M. Schmidt, *Norm form equations*, Ann. of Math. 96 (1972), 526–551.

[12] S. Sehgal, *Topics in Group Rings*, Dekker, New York, 1978.

School of Mathematics
University of East Anglia
Norwich, Norfolk NR4 7TJ, U.K.
E-mail: g.everest@uea.ac.uk

Institute of Mathematics and Informatics
Lajos Kossuth University
H-4010 Debrecen, Pf 12, Hungary
E-mail: gyory@math.klte.hu

Received on 17.9.1996 (3046)