ACTA ARITHMETICA
LXII.1 (1992)

p-primary parts of unit traces and the p-adic regulator

by

G. R. Everest* (Norwich)

Suppose K is a totally real algebraic number field with ring of algebraic integers denoted O_K. Write U_K for the group of units of O_K. The structure of U_K is known to be (see [6])

$$U_K \cong \{\pm 1\} \times \mathbb{Z}^r , \tag{1}$$

where $[K : \mathbb{Q}] = r + 1$. The trace map from K to $\mathbb{Q}$ is denoted

$$T(\mu) = \sum_{\sigma} \sigma(\mu) , \qquad \mu \in K , \tag{2}$$

the sum running over all the embeddings $\sigma : K \to \mathbb{R}$. In this paper assume further that $K/\mathbb{Q}$ is Galois, this assumption being made for technical convenience only. Suppose $\alpha \in O_K$, and $r > 1$.

Theorem. *There are asymptotic formulae as follows*:

$$T(q) = \#\{u \in U_K : |T(\alpha u)| < q\} = A(\log q)^r + O((\log q)^{r-1}) , \tag{3}$$

$$\begin{aligned} T_{p'}(q) &= \#\{u \in U_K : |T(\alpha u)| \cdot |T(\alpha u)|_p < q\} \\ &= A(\log q)^r + O((\log q)^{r-1} \log\log q) , \end{aligned} \tag{4}$$

where A denotes a positive constant (*see* (12)) *depending only on K. Here $|\ |_p$ denotes the usual p-adic absolute value, $|p|_p = p^{-1}$. So $|\ |\cdot|\ |_p$ represents the "p-primary part". In* (3) *the constant implicit in the big O notation depends only on K and α. In* (4) *it depends on p, K and α.*

Obviously, the interest in formula (4) occurs only when the following condition is satisfied:

$$\liminf_{u \in U_K} |T(\alpha u)|_p = 0 . \tag{5}$$

---

* I am grateful to Daniel Bertrand for saving me from an error in an earlier version of this paper. Also my thanks go to the referee for his helpful comments.

In this case say the orbit $T(\alpha U_K)$ is *p-unbounded*. This condition can certainly obtain. For example, in the quadratic field $\mathbb{Q}(\sqrt{5})$, the orbit $T(U_K)$ is 3 and 11-unbounded. However, it is not 31-unbounded. This represents the sum total of my knowledge of this phenomenon.

Now formula (3) can be extended to a 3-term asymptotic formula in the manner of the results in [2]. Actually, so can formula (4), and in the p-unbounded case, the error term in (4) is the correct order of magnitude.

The interest in trace values arises from the study of the norm-form equation (see [2]). Given a $\mathbb{Q}$-basis for K, $\{a_1, \ldots, a_{r+1}\}$, we obtain an equation

$$N(\boldsymbol{x}) = \prod_{\sigma:K\to\mathbb{R}} |\sigma(a_1x_1 + \ldots + a_{r+1}x_{r+1})| = a\,. \tag{6}$$

Here $\boldsymbol{x} \in \mathbb{Z}^{r+1}$ and a is a fixed, non-zero, rational number. This is called the (full) *norm-form equation*. One may study the solutions $\boldsymbol{x}$ by observing that they correspond to a finite number of orbits αU_K, and moreover, that x_i is given as $T(\beta u)$ for some $\beta \in K$, $u \in U_K$. This latter observation comes from a choice of basis, dual to the basis $\{a_1, \ldots, a_{r+1}\}$, with respect to the trace map T.

We will prove (4) in the special case that p is a prime totally split in K. In doing so we will make a study of Leopoldt's p-adic regulator. In order to get a clean proof we will assume Leopoldt's conjecture. The counting arguments are rather more delicate if Leopoldt's conjecture is false.

A lot of our interest lies with orbits of the form αG, where G is a subgroup of U_K of finite index which is p-adically homogeneous (see (27)). Using G we can get to the heart of the proof very quickly. An orbit αU_K is a finite union of such orbits so the proof of the formulae can easily be reconstructed.

There is a fairly extensive literature on the values taken by sums of (S-) units. A fundamental result in this area is contained in the paper by Evertse [3]. The results presented here build upon those in [3]; also upon other techniques developed recently (see [1], [2], [4]). At rock bottom there has to be some kind of machinery to enable one to transfer the counting of sums of units to heights of units. This is provided by the p-adic Subspace Theorem of Schlickewei (generalising the work of Schmidt), implicit in Evertse's results in [3].

In Section 1 a review is presented of formulae needed to prove (3). In Section 2 some technical lemmas are given in the form of local counting formulae and the definition of the group G is presented. In Section 3 the proof of the Theorem is given.

1. Review of counting formulae. The embeddings $\sigma : K \to \mathbb{R}$ give rise to $r + 1$ linear forms on $\mathbb{R}^r$. To see this, choose a basis for U_K modulo the group $\{\pm 1\}$ in (1), and define

$$\sigma_i(\boldsymbol{x}) = \log|\sigma_i(u(\boldsymbol{x}))|\,. \tag{7}$$

Here $u = u(\boldsymbol{x}) = e_1^{x_1}\dots e_r^{x_r}$; $\boldsymbol{x} = (x_1,\dots,x_r) \in \mathbb{Z}^r$ denoting the vector of exponents of u with respect to the chosen basis $e_1,\dots,e_r$, and $\sigma_1,\dots,\sigma_{r+1}$ denoting the distinct embeddings $\sigma_i : K \to \mathbb{R}$. Define

$$H(u) = \max_{1\le i\le r+1}\{|\sigma_i(u)|\}\,, \tag{8}$$

$$h(u) = h(\boldsymbol{x}) = \log H(u)\,, \qquad u \in U_K\,. \tag{9}$$

Here $h(\boldsymbol{x})$ is defined on $\mathbb{Z}^r$ but we consider it as a function on $\mathbb{R}^r$ by extension of scalars. The *regulator* is defined to be (see [6])

$$R_K = |\det(\sigma_i(\boldsymbol{e}_j))|\,, \qquad i = 1,\dots,r, \quad \boldsymbol{e}_j = (0,\dots,0,\underset{j}{1},0,\dots,0)\,. \tag{10}$$

It is easy to check that R_K is independent of the choices made to define it.

Theorem A (see [1], [4]).

$$U_K(q) = \#\{u \in U_K : H(u) < q\} = \frac{2(r+1)^r}{R_K r!}(\log q)^r + O((\log q)^{r-1})\,. \tag{11}$$

Write

$$A = \frac{2(r+1)^r}{R_K r!}\,. \tag{12}$$

Note. In fact $U_K(q)$ can be given as a three-term asymptotic formula (see [1]).

Define $H^*(u)$ to be the second largest member of the set of valuations considered in the definition of H ($H = H^*$ is allowed). Define, for $\theta_0 < 1$,

$$U_0 = \{u \in U_K : H^*(u)/H(u) < \theta_0\}\,. \tag{13}$$

Actually the choice of θ_0 is immaterial provided it is sufficiently small and the notation is chosen to honour this fact. See the remark in the proof of Lemma 2(ii). Define

$$U_0(q) = \#\{u \in U_0 : H(u) < q\}\,. \tag{14}$$

Lemma 1.

$$U_0(q) - U(q) = O((\log q)^{r-1})\,. \tag{15}$$

Proof. This is an easy geometric argument. It amounts to counting lattice points in a box whose sides are close to hyperplanes (take logs in (13) and use the fact that $\log H$ and $\log H^*$ are given by piecewise linear functions). ∎

Note the following asymptotic approximations for the trace map on units. Write

$$
(16)\qquad \begin{gathered} t(\mu) = \log|T(\mu)|\,, \\ t'_p(\mu) = \log(|T(\mu)|\cdot|T(\mu)|_p)\,, \qquad t_p(\mu) = \log|T(\mu)|_p\,, \end{gathered}
$$

for $\mu \in K$.

LEMMA 2. (i) *The equation* $T(\alpha u) = 0$ *has only a finite number of solutions for* $u \in U_K$.

(ii) *We have*

$$
(17)\qquad t(\alpha u) = h(u) + O(1)\,, \qquad \textit{for } u \in U_0\,,\ T(\alpha u) \neq 0\,.
$$

Here the $O(1)$ *term depends upon* α.

(iii) *Given* $\varepsilon > 0$, *there is a constant* $\lambda_1(\varepsilon, \alpha, p)$ *such that*

$$
(18)\qquad \begin{aligned} &t_p(\alpha u) > -\varepsilon h(u) - \lambda_1\,, \\ &\left.\begin{matrix} t(\alpha u) \\ t'_p(\alpha u) \end{matrix}\right\} > (1-\varepsilon)h(u) - \lambda_1 \qquad \textit{for all } u \in U_K \textit{ with } T(\alpha u) \neq 0\,. \end{aligned}
$$

Note. In view of (i) assume always that $T(\alpha u) \neq 0$. The finitely many exceptions to this clearly do not affect the type of results given in this paper.

Proof. (i) and (iii). Theorem 2 of Evertse in [3] gives

$$
T(\alpha u) = 0 \qquad \text{only finitely often,}
$$

and

$$
\begin{gathered} t_p(\alpha u) > -\varepsilon h(u) - \lambda_1\,, \\ \left.\begin{matrix} t(\alpha u) \\ t'_p(\alpha u) \end{matrix}\right\} > (1-\varepsilon)h(u) - \lambda_1\,, \end{gathered}
$$

for $0 < \varepsilon < 1$ and $0 < \lambda_1 = \lambda_1(K, p, \varepsilon, \alpha)$, provided there is no vanishing sub-sum of $T(\alpha u)$. That is,

$$
\sum_{j=1}^{t} \sigma_{i_j}(\alpha u) \neq 0 \qquad \forall \{i_1, \ldots, i_t\} \subset \{1, \ldots, r+1\}\,.
$$

If $K/\mathbb{Q}$ is Galois then a vanishing sub-sum implies, upon application of all the elements of the Galois group and summing, that

$$
t \sum_{\sigma} \sigma(\alpha u) = 0\,.
$$

Thus a sub-sum can vanish only if the whole sum has vanished.

Note. For the non-Galois case a bound is possible in part (iii) but it requires quite a detour into an application of the p-adic Subspace Theorem.

(ii) This follows directly from the definition of U_0. Notice that the choice of θ_0 depends on α. It must be taken so that one of the terms in the sum for $T(\alpha u)$ is dominant. ∎

Finally, in this section, note the effect upon all that we have said, of replacing U_K by a subgroup of finite index. Suppose $G \triangleleft U_K$.

THEOREM B (see [1]).

$$G(q) = \#\{u \in G : H(u) < q\} = B(\log q)^r + O((\log q)^{r-1}), \tag{19}$$

where B depends upon r, R_K and $[U_K : G]$.

Also define

$$G_0 = G \cap U_0 \quad \textit{and} \quad G_0(q) = \#\{u \in G_0 : H(u) < q\}. \tag{20}$$

Then (compare with (15))

$$G_0(q) - G(q) = O((\log q)^{r-1}). \tag{21}$$

2. Local counting. In this section we will define the p-adic homogeneous hull of U_K, and obtain counting formulae for elements whose trace has fixed p-part. Suppose $p > r + 1$ is totally split and interpret this in the following way. Suppose there exist embeddings

$$\tau_i : K \to \mathbb{Q}_p, \quad i = 1, \dots, r+1, \tag{22}$$

these coming from the prime ideals lying above p. The *group of* 1-*units of* U_K is defined as

$$U_1 = \{u \in U_K : \tau_i(u) \equiv 1 \bmod p,\ 1 \le i \le r+1\}. \tag{23}$$

Then U_1 is of finite index in U_K so choose a basis $\{e_1, \dots, e_r\}$ for this group. Recall the definition of Leopoldt's *p-adic regulator*:

$$|R_p| = \det(\log_p \tau_i(e_j)), \quad 1 \le i, j \le r, \tag{24}$$

where $\log_p$ denotes the usual p-adic logarithm on $1 + p\mathbb{Z}_p$. Leopoldt has conjectured that $|R_p| \ne 0$ and this is known to be true for abelian extensions $K/\mathbb{Q}$ (see [5]) but for only a few non-abelian extensions. See Leopoldt's original paper [7].

Suppose Leopoldt's conjecture is true. The matrix R_p is equivalent to a matrix in Smith Normal Form. Choose unimodular matrices T and S (over $\mathbb{Z}_p$), with

$$TR_pS = \begin{bmatrix} p^{f_1} & & 0 \\ & \ddots & \\ 0 & & p^{f_r} \end{bmatrix}, \quad f_1 \le \dots \le f_r,\ f_i \in \mathbb{N}. \tag{25}$$

Multiply on the right by

$$S' = \begin{bmatrix} p^{f_r - f_1} & & 0 \\ & \ddots & \\ 0 & & p^{f_r - f_r} \end{bmatrix}.$$

Now reduce the matrix $SS' \bmod p^{f_r+1}$. We always identify $\mathbb{Z}/p^N\mathbb{Z}$ with $\mathbb{Z}_p/p^N\mathbb{Z}_p$. This means we have found an integer matrix S'' which effects the replacement of the set $\{e_1, \ldots, e_r\}$ by a set $\{g_1, \ldots, g_r\}$ with the following property: the matrix

$$(\log_p \tau_i(g_j)) \tag{26}$$

has Smith Normal Form equal to $\operatorname{diag}(p^f, \ldots, p^f)$, $f = f_r$.

Define the group G to be

$$G = \langle g_1, \ldots, g_r \rangle\,, \tag{27}$$

the *p-adic homogeneous hull* of U_K. We say G is *p-adically homogeneous*. Notice that the matrix S'' is non-singular so the group G is certainly of finite index inside U_1, hence in U_K.

Given $m \in \mathbb{Q}$, write $m = p^s a$, where $p \nmid a \in \mathbb{Q}$. Then $\operatorname{ord}_p m$ denotes s, as usual.

Given $\alpha \in O_K$ we aim to study the solvability of the equation

$$\operatorname{ord}_p T(\alpha u) = t\,, \qquad t \in \mathbb{N}\,, \tag{28}$$

for $u \in G$. We will see that the orbit αG is p-unbounded provided α satisfies

$$\tau_i(\alpha) \not\equiv 0 \bmod p\,, \quad i = 1, \ldots, r+1 \quad \text{and} \quad T(\alpha) \equiv 0 \bmod p^f\,. \tag{29}$$

N o t e. Given G it is an easy exercise to show that infinitely many $\alpha \in O_K$ exist with property (29).

Write (28) in the form

$$T(\alpha u) \equiv \omega p^t \bmod p^{t+1} \qquad \text{with } \omega \in \mathbb{F}_p^*\,.$$

That is,

$$\alpha_1 u_1 + \ldots + \alpha_r u_r + \alpha_{r+1} u_{r+1} \equiv \omega p^t \bmod p^{t+1}\,, \tag{30}$$

where $\alpha_i = \tau_i(\alpha)$, $u_i = \tau_i(u)$, $\omega \in \mathbb{F}_p^*$, $t \in \mathbb{N}$. We may suppose that $N_{K|\mathbb{Q}}(u) = 1$, $\forall u \in G$, to ease the computations. Then (30) becomes

$$\alpha_1 v_1 + \ldots + \alpha_r v_r + \alpha_{r+1} \equiv \omega' p^t \bmod p^{t+1}\,, \qquad \omega' \in \mathbb{F}_p^*\,, \tag{31}$$

where the v_i are defined by

$$v_i = u_1 \ldots u_i^2 \ldots u_r\,. \tag{32}$$

Taking p-adic logarithms gives a matrix equation

$$\begin{bmatrix} 2 & 1 & & 1 \\ & 2 & & \\ & & \ddots & \\ 1 & & & 2 \end{bmatrix} \begin{bmatrix} \log_p u_1 \\ \vdots \\ \log_p u_r \end{bmatrix} = \begin{bmatrix} \log_p v_1 \\ \vdots \\ \log_p v_r \end{bmatrix}. \tag{33}$$

Also, remembering (27) and taking p-adic logs,

$$\begin{bmatrix} \log_p \tau_1(g_1) & \ldots & \log_p \tau_1(g_r) \\ \ldots & \ldots & \ldots \\ \log_p \tau_r(g_1) & \ldots & \log_p \tau_r(g_r) \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} = \begin{bmatrix} \log_p u_1 \\ \vdots \\ \log_p u_r \end{bmatrix}. \tag{34}$$

Notice that the matrix with 2's and 1's is invertible if $p > r + 1$, so find invertible matrices U and V over $\mathbb{Z}_p$ with

$$U \begin{bmatrix} p^f & & 0 \\ & \ddots & \\ 0 & & p^f \end{bmatrix} V\boldsymbol{x} = \begin{bmatrix} \log_p v_1 \\ \vdots \\ \log_p v_r \end{bmatrix}. \tag{35}$$

Finally, write

$$U^{-1} \begin{bmatrix} \log_p v_1 \\ \vdots \\ \log_p v_r \end{bmatrix} = \begin{bmatrix} \log_p \omega_1 \\ \vdots \\ \log_p \omega_r \end{bmatrix}, \quad \text{and} \quad V\boldsymbol{x} = \boldsymbol{y}. \tag{36}$$

Let $N(t)$ denote the number of solutions $\boldsymbol{x} \in (\mathbb{Z}/p^{t+1-f}\mathbb{Z})^r = (\mathbb{Z}_p/p^{t+1-f}\mathbb{Z}_p)^r$ of the equations (31), (32), (34).

LEMMA 3. *Suppose condition* (29) *is satisfied for* $\alpha \in O_K$. *Then*

$$N(t) = \begin{cases} 0, & t < f, \\ (p-1)p^{(t+1-f)(r-1)}, & t \geq f. \end{cases} \tag{37}$$

Proof. In order that (35) and (36) be satisfied for $\boldsymbol{y} \in \mathbb{Z}_p^r$, we must have

$$\omega_i \equiv 1 \bmod p^f, \quad i = 1, \ldots, r. \tag{38}$$

Assume this is the case, and write

$$\omega_i = 1 + p^f z_i, \quad z_i \in \mathbb{Z}_p, \quad i = 1, \ldots, r. \tag{39}$$

In terms of (36), the congruence at (31) becomes

$$\alpha_1 \omega_1^{u_{11}} \ldots \omega_r^{u_{1r}} + \ldots + \alpha_r \omega_1^{u_{r1}} \ldots \omega_r^{u_{rr}} + \alpha_{r+1} \equiv \omega' p^t \bmod p^{t+1}, \tag{40}$$

where the matrix U (see (35)) is given as

$$U = (u_{ij}), \quad u_{ij} \in \mathbb{Z}_p. \tag{41}$$

It is clear already, by reducing $\bmod p^f$, that no solution of (40) exists if $t < f$. The proof of the lemma will follow by assigning arbitrary values

$\bmod p^{t+1-f}$ to $r-1$ of the z_i in (39) (also to $\omega \in \mathbb{F}_p^*$, see (30)). Then the congruence (40) is solved uniquely for the other z_i (hence ω_i). This obviously gives the formula required.

To justify this last statement, an argument like Hensel's Lemma is required. The conditions at (29) imply that for some j with $1 \le j \le r$, we have

$$\alpha_1 u_{1j} + \alpha_2 u_{2j} + \ldots + \alpha_r u_{rj} \not\equiv 0 \bmod p\,. \tag{42}$$

If this were not so then the equation

$$U\boldsymbol{\alpha} = 0 \bmod p, \qquad \boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r), \tag{43}$$

would have a non-trivial solution. But U reduces $\bmod p$ to a non-singular matrix. So (42) is certainly justified, let us say $j = 1$.

Now assign arbitrary values $\bmod p^{t+1-f}$ to $z_2, \ldots, z_r$. The condition (42) is precisely the condition that guarantees a unique solution of (40) for z_1, hence ω_1. This is a standard argument (à la Hensel). The coefficients of the p-adic expansion for z_1 are found by induction, condition (42) guaranteeing uniqueness. The proof of the lemma is complete. ∎

On the group G there is a filtration obtained as follows. Every $u \in G$ satisfies

$$\tau_i(u) \equiv 1 \bmod p^f, \qquad i = 1, \ldots, r+1\,.$$

Given $t \ge f$ define

$$G_t = \{u \in G : \tau_i(u) \equiv 1 \bmod p^t\}\,. \tag{44}$$

Lemma 4. *For $t \ge f$,*

$$G_t = G^{p^{t-f}}\,. \tag{45}$$

Proof. The question is simply this: what is the general solution of the congruence

$$(\log_p \tau_i(g_j))\boldsymbol{x} \equiv \mathbf{0} \bmod p^t\ ?$$

Taking the Smith Normal Form it is obvious that $\boldsymbol{x} \in \mathbb{Z}^r$ is a solution if and only if $p^{t-f} \mid x_i,\ i = 1, \ldots, r$. ∎

This is important. Fix $N(t)$ solutions of the equation

$$\mathrm{ord}_p\, T(\alpha u) = t\,,$$

for $u \bmod G_{t+1}$, say $u_1, \ldots, u_{N(t)}$. Here the vector of exponents of u_j with respect to the basis $\{g_1, \ldots, g_r\}$ (see (27)) is given $\bmod (p^{t+1-f}\mathbb{Z})^r$. The set of all the solutions is precisely the collection of orbits

$$u_j G_{t+1}\,, \qquad j = 1, \ldots, N(t)\,. \tag{46}$$

So far we have studied the congruence (28) for $t \ge f$ and for $u \in G$. In order that the Theorem may be proved, this being a statement about

$u \in U_K$, we need to put the result together from results about $u \in G$. So notice the following.

LEMMA 5. *Suppose* $\alpha \in O_K$ *satisfies*

$$\operatorname{ord}_p T(\alpha) = \theta \quad \textit{for } \theta < f\,. \tag{47}$$

Then the equation (28) *has a solution only for* $t = \theta$ *but for any* $u \in G$. ∎

This is an obvious statement but it is clear that the Theorem follows from the corresponding results about orbits αG, for $\alpha \in O_K$. Suppose, in fact, we wanted to study an orbit γU_K for some $\gamma \in O_K$, $\tau_i(\gamma) \not\equiv 0 \bmod p$ for all $i = 1, \ldots, r+1$. Choosing coset representatives turns this into a finite number of orbits of the kind αG. Each of these is either p-bounded or not and Lemmas 3 and 5 give precise criteria to determine which of the two possibilities applies.

In the next section we will run through the counting arguments in the p-unbounded case.

3. Proof of Theorem. Given $\alpha \in O_K$ with $\tau_i(\alpha) \not\equiv 0 \bmod p$ for each i, suppose the orbit αG is p-unbounded. We agree to identify $u \in G$ with $\boldsymbol{x} \in \mathbb{Z}^r$ via the basis $\{g_1, \ldots, g_r\}$. Also, for all $t \geq f$, identify G_t with $G^{p^{t-f}}$, using (45). This transforms the counting of units to the counting of lattice points inside regions of $\mathbb{R}^r$.

The proof of (3) will act as a dummy run for the proof of (4). Write $(\log q = Q)$

$$\begin{aligned} t(Q) &= \#\{u \in U_K : t(\alpha u) < Q\} \\ &= \#\{u \in U_0 : t(\alpha u) < Q\} + \#\{u \in U_K - U_0 : t(\alpha u) < Q\}\,. \end{aligned} \tag{48}$$

For the second bracket in (48), apply (18) to deduce that this expression is

$$O(\#\{u \in U_K - U_0 : (1-\varepsilon)h(u) - \lambda_1 < Q\})\,. \tag{49}$$

Now apply (15) to deduce that (49) lies in the error term.

Going back to the first term in (48), apply (17) to get

$$\#\{u \in U_0 : h(u) + O(1) < Q\}\,. \tag{50}$$

The result follows by applying (15) and (11). ∎

Now suppose that $\alpha \in O_K$ and, with the notation of Section 2, $\tau_i(\alpha) \not\equiv 0 \bmod p$ for $i = 1, \ldots, r+1$. Suppose that the orbit αG is p-unbounded and count

$$\begin{aligned} t_p'(Q) &= \#\{u \in G : t_p'(\alpha u) < Q\} \\ &= \#\{u \in G : t(\alpha u) + t_p(\alpha u) < Q\}\,. \end{aligned} \tag{51}$$

If we do the same trick as at (48) we may assume that $u \in G_0$. Those outside give a contribution only in the error. Thus (51) becomes the simpler expression

$$\#\{u \in G_0 : h(u) + t_p(u) < Q\}\,. \tag{52}$$

The object we really want to study is

$$\#\{u \in G : h(u) + t_p(u) < Q\}\,. \tag{53}$$

This differs from (52) by an amount which is

$$\#\{u \in G - G_0 : h(u) + t_p(u) < Q\}\,. \tag{54}$$

We claim that the expression in (54) already lies in the error, leaving us free to study (53), as we wish. To see this, apply (18) to obtain

$$(1-\varepsilon)h(u) - \lambda_1 < h(u) + t_p(u) < Q\,.$$

Thus (54) is majorised by (rechoose $\varepsilon > 0$ if necessary)

$$\#\{u \in G - G_0 : h(u) < (1+\varepsilon)Q\}\,. \tag{55}$$

The condition that $u \notin G_0$ amounts to (see (13))

$$h^*(u) \le h(u) \le h^*(u) + \lambda_2\,, \tag{56}$$

where $h^* = \log H^*$, and λ_2 is constant.

Applying (55) means we now estimate

$$\#\{u \in G : h(u) < (1+\varepsilon)Q,\ |h(u) - h^*(u)| < \lambda_2\}\,. \tag{57}$$

But this amounts to the same idea as that in Lemma 1. The element $u \in G$ is identified with $\boldsymbol{x} \in \mathbb{Z}^r$ via the choice of basis. The functions h and h^* are piecewise linear functions of $\boldsymbol{x}$ so, as before, we are counting lattice points inside a large box (this time of side $(1+\varepsilon)Q$) which lie close to a finite number of hyperplanes. Thus we obtain

$$\#\{u \in G - G_0 : h(u) + t_p(u) < Q\} = O(Q^{r-1})\,.$$

As claimed, the problem is reduced to the study of (53).

Recall the remarks at (46) in Section 2. Use the filtration

$$G \ge G_f \ge G_{f+1} \ge \ldots$$

In terms of the notation in Section 2, (53) becomes

$$\sum_{t=f}^{\infty} \sum_{j=1}^{N(t)} \#\{v \in G_{t+1} : h(u_j v) < Q + t\log p\}\,. \tag{58}$$

It is clear by applying (18) that the upper range of t is restricted. In fact,

$$(1-\varepsilon)h(u) - \lambda_1 < t_p'(\alpha u) \le h(u) - t\log p < Q + \lambda_3 \tag{59}$$

implies

$$t\log p < \varepsilon h(u) + \lambda_4\,. \tag{60}$$

Now (59) and (60) give

$$t < \frac{\varepsilon Q + \lambda_5}{(1-\varepsilon)\log p}\,.$$

Rechoosing $\varepsilon > 0$ gives

$$t < \varepsilon Q\,. \tag{61}$$

This is a little too large to be practical so now we introduce the p-adic analogue of the trick at (48).

Given $u \in G$ with $u = u_j v$ as above, write $G_p(t)$ for those u with

$$h(u_j) > p^{t/2}\,. \tag{62}$$

Then formula (18) gives

$$p^{t/2} < h(u_j) < \frac{Q + \lambda_6}{1-\varepsilon}\,,$$

where the right hand inequality comes by applying (59) directly. Now taking logs gives a much smaller upper bound for t. To summarize, let T denote the maximum value of t allowed. Then

$$T < \begin{cases} 2\log Q/\log p + \lambda_7, & u \in G_p(t),\\ \varepsilon Q, & u \in G. \end{cases} \tag{63}$$

Write $T' = 2\log Q/\log p + \lambda_7$, assumed to be an integer. Define

$$N(t, G) = \#\{u \in G : t_p(u) = -t\log p,\ h(u) < Q + t\log p\}\,.$$

Then

$$t'_p(Q) = \sum_{t=f}^{T} N(t, G) = \sum_{t=f}^{T'} N(t, G_p(t)) + \sum_{t=f}^{T} N(t, G - G_p(t))\,.$$

Notice that if $t > T'$ then u cannot be in any $G_p(t)$. Hence

$$t'_p(Q) = \sum_{t=f}^{T'} N(t, G) + \sum_{t=T'}^{T} N(t, G - G_p(t)) = S_1 + S_2\,. \tag{64}$$

We claim that S_2 lies in the error term. First show that S_1 gives the formula claimed. Expand in the manner of (58):

$$\sum_{t=f}^{T'} \sum_{j=1}^{N(t)} \#\{v \in G_{t+1} : h(u_j v) < Q + t\log p\}\,.$$

Use (45), together with (27), to obtain

$$\sum_{t=f}^{T'} \sum_{j=1}^{N(t)} \#\{\boldsymbol{v} \in \mathbb{Z}^r : h(\boldsymbol{u}_j + p^{t+1-f}\boldsymbol{v}) < Q + t\log p\}\,, \tag{65}$$

where we identify elements of G with their vectors of exponents with respect to the basis in (27). Divide through by p^{t+1-f} so that each $p^{f-t-1}\boldsymbol{u}_j \in C_0$, the unit cube about the origin in $\mathbb{R}^r$. We have remarked already, after (9), that h is defined on $\mathbb{R}^r$. Observe that for any $\boldsymbol{\delta} \in C_0$,

$$h(\boldsymbol{v}+\boldsymbol{\delta}) = h(\boldsymbol{v}) + O(1) \quad \text{for } \boldsymbol{v} \in \mathbb{Z}^r\,,$$

where the constant implicit in big O is uniform and depends only upon K. Then (65) becomes

$$\sum_{t=f}^{T'} \sum_{j=1}^{N(t)} \#\Big\{\boldsymbol{v} \in \mathbb{Z}^r : h(\boldsymbol{v}) < \frac{Q + t\log p}{p^{t+1-f}} + \lambda_8\Big\}\,.$$

More simply,

$$\sum_{t=f}^{T'} \sum_{j=1}^{N(t)} \#\Big\{\boldsymbol{v} \in \mathbb{Z}^r : h(\boldsymbol{v}) < \frac{Q}{p^{t+1-f}} + \lambda_9\Big\}\,.$$

So we are back to counting elements of G again. Formula (19) applies to give

$$\begin{aligned}(66)\quad \sum_{t=f}^{T'} \sum_{j=1}^{N(t)} &\Big\{B\Big(\frac{Q}{p^{t+1-f}} + \lambda_9\Big)^r + O\Big(\Big(\frac{Q}{p^{t+1-f}}\Big)^{r-1}\Big)\Big\} \\ &= \sum_{t=f}^{T'} B(p-1)p^{(t+1-f)(r-1)} \frac{Q^r}{p^{(t+1-f)r}} + O\Big(\sum_{t=f}^{T'} Q^{r-1}\Big) \\ &= BQ^r(p-1)\sum_{t=f}^{T'} \frac{1}{p^{t+1-f}} + O(Q^{r-1}\log Q)\,,\end{aligned}$$

using formula (37) and (63). The sum in the first term differs from $(p-1)^{-1}$ by an amount which is

$$O(p^{-T'}) = O(p^{-2\log Q/\log p}) = O(Q^{-2})\,.$$

So (66) comes out to be

$$BQ^r + O(Q^{r-1}\log Q)\,,$$

as we require.

Now go back to (64) and show that S_2 lies in the error. Filtering as before we see that S_2 is majorised by

$$(67)\quad \sum_{t=T'}^{T} \sum_{j=1}^{N(t)} \#\{\boldsymbol{v} \in \mathbb{Z}^r : h(\boldsymbol{u}_j) \le p^{t/2},\ h(\boldsymbol{u}_j + p^{t+1-f}\boldsymbol{v}) < Q + t\log p\}\,.$$

Divide through by p^{t+1-f} as before. Also notice that a crude upper bound for the number of j with $h(\boldsymbol{u}_j) \le p^{t/2}$ is given by $O(p^{tr/2})$. So replace (67) by

$$\sum_{t=T'}^{T} p^{tr/2} \# \left\{ \boldsymbol{v} \in \mathbb{Z}^r : h(\boldsymbol{v} + p^{f-t-1}\boldsymbol{u}_j) < \frac{Q + t\log p}{p^{t+1-f}} \right\}.$$

The vectors $p^{f-t-1}\boldsymbol{u}_j$ are shrinking:

$$|p^{f-t-1}\boldsymbol{u}_j| < p^{-t/2} \qquad (|\ | \text{ denoting vector norm}).$$

Therefore S_2 is majorised by

$$\sum_{t=T'}^{T} p^{tr/2} \# \left\{ \boldsymbol{v} \in \mathbb{Z}^r : h(\boldsymbol{v}) < \frac{Q}{p^t} + \frac{\lambda_{10}}{p^{t/2}} \right\}. \tag{68}$$

Recall the sizes of T' and T given at (63). Expand out to obtain

$$O\biggl(\sum_{t=T'}^{T} \frac{Q^r}{p^{tr/2}}\biggr) + O\biggl(\sum_{t=T'}^{T} \frac{Q^{r-1}}{p^{t(r-1)/2}}\biggr). \tag{69}$$

Now $p^{-T'/2}$ is $O(Q^{-1})$. Putting this into the expressions in (69) shows they are very small indeed. ∎

References

[1] G. R. Everest, *Uniform distribution and lattice point counting*, J. Austral. Math. Soc., to appear.

[2] —, *On the solution of the norm-form equation*, Amer. J. Math., to appear.

[3] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. 53 (1984), 225–244.

[4] K. Győry and A. Pethő, *Über die Verteilung der Lösungen von Normformen Gleichungen, III*, Acta Arith. 37 (1980), 143–165.

[5] N. Koblitz, *p-Adic Analysis: A Short Course on Recent Work*, London Math. Soc. Lecture Note Ser. 46, Cambridge Univ. Press, 1980.

[6] S. Lang, *Algebraic Number Theory*, Addison-Wesley, New York 1970.

[7] H. W. Leopoldt, *Eine p-adische Theorie der Zetawerte II*, J. Reine Agnew. Math. 274/275 (1975), 224–239.

SCHOOL OF MATHEMATICS
UNIVERSITY OF EAST ANGLIA
NORWICH NR4 7TJ, U.K.

Received on 12.3.1991
and in revised form on 26.7.1991 (2126)