Multivariate Diophantine equations with many solutions

J.-H. Evertse, P. Moree, C.L. Stewart and R. Tijdeman

1 Introduction

Among other things we show that for each n-tuple of positive rational numbers $(a_1, \dots, a_n)$ there are sets of primes S of arbitrarily large cardinality s such that the solutions of the equation $a_1x_1 + \cdots + a_nx_n = 1$ with $x_1, \dots, x_n$ S-units are not contained in fewer than $\exp((4+o(1))s^{1/2}(\log s)^{-1/2})$ proper linear subspaces of $\mathbb{C}^n$. This generalizes a result of Erdős, Stewart and Tijdeman [6] for S-unit equations in two variables.
Further, we prove that for any algebraic number field K of degree n, any integer m with $1 \leq m < n$, and any sufficiently large s there are integers $\alpha_0, \dots, \alpha_m$ in K which are linearly independent over $\mathbb{Q}$, and prime numbers $p_1, \dots, p_s$, such that the norm polynomial equation

$$|N_{K/\mathbb{Q}}(\alpha_0 + \alpha_1x_1 + \cdots + \alpha_mx_m)| = p_1^{z_1} \cdots p_s^{z_s}$$

has at least $\exp\{(1 + o(1))\frac{n}{m}s^{m/n}(\log s)^{-1+m/n}\}$ solutions in $x_1, \dots, x_m$, $z_1, \dots, z_s \in \mathbb{Z}$. This generalizes a result of Moree and Stewart [18] for $m = 1$.
Our main tool, also established in this paper, is an effective lower bound for the number $\psi_{K,T}(X, Y)$ of ideals in a number field K of norm $\leq X$ composed of prime ideals which lie outside a given finite set of prime ideals T and which have norm $\leq Y$. This generalizes results of Canfield, Erdős and Pomerance [5] and of Moree and Stewart [18].

---

[1]The research of C.L. Stewart was supported in part by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.
[2]*2000 Mathematics Subject Classification:* 11D57, 11D61
[3]*Keywords and phrases:* S-unit equations, norm form equations, smooth numbers

2 Results

Let $S = \{p_1, \ldots, p_s\}$ be a set of prime numbers. We call a rational number an S-unit if both the denominator and the numerator of its simplified representation are composed of primes from S. Evertse [7] proved that for any non-zero rational numbers a, b, the equation $ax + by = 1$ in S-units x, y has at most $\exp(4s + 6)$ solutions. On the other hand, Erdős, Stewart and Tijdeman [6] showed that equations of this type can have as many as $\exp\{(4 + o(1))(s/\log s)^{1/2}\}$ such solutions as $s \to \infty$. Thus the dependence on s cannot be polynomial. In the present paper we generalise this result to S-unit equations in an arbitrary number n of variables. Here n is considered to be given.

In [8] Evertse proved that for given non-zero rational numbers $a_1, \ldots, a_n$, the equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 1 \quad \text{in } S\text{-units } x_1, x_2, \ldots, x_n \tag{2.1}$$

has at most $(2^{35}n^2)^{n^3(s+1)}$ non-degenerate solutions. We call a solution degenerate if there is some non-empty proper subset $\{i_1, \ldots, i_k\}$ of $\{1, \ldots, n\}$ such that $a_{i_1}x_{i_1} + a_{i_2}x_{i_2} + \cdots + a_{i_k}x_{i_k} = 0$ and otherwise non-degenerate. In [9], Evertse, Győry, Stewart and Tijdeman showed that there are equations (2.1) which have as many as $\exp\{(4+o(1))(s/\log s)^{1/2}\}$ non-degenerate solutions as $s \to \infty$ and subsequently Granville [10] improved this to $\exp(c_0 s^{1-1/n}(\log s)^{-1/n})$ for a positive number c_0. For our first result we shall establish a version of Granville's theorem with c_0 given explicitly.

THEOREM 1. *Let ε be a positive real number and let $a_1, \ldots, a_n$ be non-zero rational numbers. There exists a positive number s_0, which is effectively computable in terms of ε and $a_1, \ldots, a_n$, with the property that for every integer $s \geq s_0$ there is a set of primes S of cardinality s such that equation* (2.1) *has at least*

$$\exp\left\{(1-\varepsilon)\tfrac{n^2}{n-1}s^{1-1/n}(\log s)^{-1/n}\right\}$$

non-degenerate solutions in S-units $x_1, x_2, \ldots, x_n$.

Theorem 1 does not exclude the possibility that the sets of solutions of the equations (2.1) under consideration are of a special shape, for instance that they are contained in the union of a small number of proper linear subspaces of $\mathbb{Q}^n$ or in some algebraic variety of small degree. We shall prove in Theorem 2 that this is not the case.

Let again S be a set of primes and $\mathbf{a} = (a_1, \ldots, a_n)$ a tuple of non-zero rational numbers. Recall that the total degree of a polynomial P is the maximum of the sums $k_1 + \cdots + k_n$ taken over all monomials $X_1^{k_1} \cdots X_n^{k_n}$ occurring in P. Define $g(\mathbf{a}, S)$ to be the smallest integer g with the following property: there exists a polynomial $P \in \mathbb{C}[X_1, \ldots, X_n]$ of total degree g, not divisible by $a_1X_1 + \cdots + a_nX_n - 1$, such that

$$P(x_1, \ldots, x_n) = 0 \quad \text{for every solution } (x_1, \ldots, x_n) \text{ of (2.1).} \tag{2.2}$$

For instance, suppose that the set of solutions of (2.1) is contained in the union of t proper linear subspaces of $\mathbb{C}^n$, given by equations $c_{i1}X_1 + \cdots + c_{in}X_n = 0$ $(i = 1, \ldots, t)$, say. Then (2.2) is satisfied by $P = \prod_{i=1}^{t}(\sum_{j=1}^{n} c_{ij}X_j)$ which is not divisible by $a_1X_1 + \cdots + a_nX_n - 1$; hence $t \geq g(\mathbf{a}, S)$. This means that if $g(\mathbf{a}, S)$ is large, the set of solutions of (2.1) cannot be contained in the union of a small number of proper linear subspaces of $\mathbb{C}^n$. Likewise, the set of solutions of (2.1) cannot be contained in a proper algebraic subvariety of small degree of the variety given by (2.1). Our precise result is as follows.

THEOREM 2. *Let ε be a positive real number and let $\mathbf{a} = (a_1, \ldots, a_n)$ be an n-tuple of non-zero rational numbers. There exists a positive number s_1, which is effectively computable in terms of ε and $\mathbf{a}$, with the property that for every integer $s \geq s_1$ there is a set of primes S of cardinality s such that*

$$g(\mathbf{a}, S) \geq \exp\left\{(4 - \varepsilon)s^{1/2}(\log s)^{-1/2}\right\}.$$

Note that for $n = 2$, both Theorems 1 and 2 imply the above mentioned result of Erdős, Stewart and Tijdeman.

We prove results analogous to Theorems 1 and 2 for "norm polynomial equations."

In what follows, K is an algebraic number field. We denote by O_K the ring of integers of K. Let $\alpha_0, \ldots, \alpha_m$ be elements of O_K which are linearly independent over $\mathbb{Q}$ and for which $\mathbb{Q}(\alpha_0, \ldots, \alpha_m) = K$. Further, let $p_1, \ldots, p_s$ be distinct prime numbers. From results of Schmidt [20] and Schlickewei [19], it follows that the *norm form equation*

$$|N_{K/\mathbb{Q}}(\alpha_0x_0 + \cdots + \alpha_mx_m)| = p_1^{z_1} \cdots p_s^{z_s} \tag{2.3}$$

has only finitely many solutions in integers $x_0, \ldots, x_m,\ z_1, \ldots, z_s$ with $\gcd(x_0, \ldots, x_m) = 1$ if and only if the left-hand side satisfies some suitable non-degeneracy condition. Instead of (2.3) we deal with *norm polynomial equations*

$$|N_{K/\mathbb{Q}}(\alpha_0+\alpha_1x_1+\cdots+\alpha_mx_m)|=p_1^{z_1}\cdots p_s^{z_s} \quad \text{in } x_1,\ldots,x_m,\, z_1,\ldots,z_s\in\mathbb{Z}, \tag{2.4}$$

that is, norm form equations with $x_0=1$. As it turns out, the number of solutions of equation (2.4) is finite if $\alpha_0,\ldots,\alpha_m$ are linearly independent over $\mathbb{Q}$. Under this hypothesis, Bérczes and Győry ([2, Theorem 2, Corollary 8] or [1, Chapter 1]) proved that equation (2.4) has at most

$$\left(2^{17}n\right)^{\delta(m)(s+1)}$$

solutions, where $n=[K:\mathbb{Q}]$ and $\delta(m)=\frac{2}{3}(m+1)(m+2)(2m+3)-4$. In fact, this is a consequence of a much more general result of theirs on decomposable polynomial equations.

Note that for $m=1$, equation (2.4) is just the generalised Ramanujan-Nagell equation

$$|f(x)|=p_1^{z_1}\cdots p_s^{z_s} \quad \text{in } x,z_1,\ldots,z_s\in\mathbb{Z}, \tag{2.5}$$

where f is an irreducible polynomial in $\mathbb{Z}[X]$ of degree at least 2. Erdős, Stewart and Tijdeman [6] proved that given any $n\geq 2$ and any sufficiently large integer s there are a polynomial $f\in\mathbb{Z}[X]$ of degree n and primes $p_1,\ldots,p_s$ such that (2.5) has more than $\exp\{(1+o(1))n^2s^{1/n}(\log s)^{(1/n)-1}\}$ solutions. The polynomial constructed by Erdős, Stewart and Tijdeman splits into linear factors over $\mathbb{Q}$.

Subsequently Moree and Stewart [18] proved a similar result in which the constructed polynomial f is irreducible. More precisely, let K be a field of degree n over $\mathbb{Q}$ and let f be a monic irreducible polynomial in $\mathbb{Z}[X]$ of degree n such that a root of f generates K over $\mathbb{Q}$. Let $\pi_f(x)$ denote the number of primes p with $p\leq x$ for which $f(x)\equiv 0 \pmod p$ has a solution. It follows from the Chebotarev density theorem (see Theorems 1.3 and 1.4 of [13]) that

$$\pi_f(x)=\frac{1}{c_K}(1+o(1))\frac{x}{\log x},$$

where c_K is a positive number which depends on K only. Let L denote the normal closure of K. Then c_K equals $[L:\mathbb{Q}]$ divided by the number of field automorphisms of $L/\mathbb{Q}$ that fix at least one root of f, or in group theoretic terms, $c_K=\#G/\#(\cup_{\sigma\in G}\sigma H\sigma^{-1})$, where $H=\mathrm{Gal}(L/K)$ and $G=\mathrm{Gal}(L/\mathbb{Q})$, see [3, Theorem 2]. Thus $1\leq c_K\leq n$ is a rational number and if K is normal then $c_K = n$. Moree and Stewart [18] proved that for each field K of degree n over $\mathbb{Q}$ there is a polynomial f, as above, such that the number of solutions of (5) is $\exp\{(1+o(1))n(c_K s)^{1/n}(\log s)^{1/n-1}\}$.

We generalize the result of Moree and Stewart to norm polynomial equations as follows.

Theorem 3. *Let K be an algebraic number field of degree $n \geq 2$. Let $\alpha_1, \ldots, \alpha_m$ be elements of O_K which are linearly independent over $\mathbb{Q}$ where $1 \leq m \leq n-1$. Let $\varepsilon > 0$. There exists a positive number s_2 which is effectively computable in terms of ε, K and $\alpha_1, \ldots, \alpha_m$, with the property that for every integer $s \geq s_2$ there are a set $S = \{p_1, \ldots, p_s\}$ of rational prime numbers and a number α_0 with*

$$\text{(2.6)} \qquad \alpha_0 \in O_K,\ \mathbb{Q}(\alpha_0) = K,\ \alpha_0\ \mathbb{Q}\text{-linearly independent of } \alpha_1, \ldots, \alpha_m,$$

such that equation (2.4) *has more than*

$$\exp\{(1-\varepsilon)\tfrac{n}{m}(c_K s)^{m/n}(\log s)^{(m/n)-1}\}$$

solutions.

Given a set of primes $S = \{p_1, \ldots, p_s\}$ and a tuple $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n)$ of elements of O_K, we define $g(\boldsymbol{\alpha}, S)$ to be the smallest integer g with the following property: there exists a non-identically zero polynomial $P \in \mathbb{C}[X_1, \ldots, X_m]$ of total degree g such that

$$\text{(2.7)} \qquad P(x_1, \ldots, x_m) = 0$$
$$\text{for every solution } (x_1, \ldots, x_m,\ z_1, \ldots, z_s) \text{ of (2.4).}$$

We prove the following result.

Theorem 4. *Let $K, n, m,\ \alpha_1, \ldots, \alpha_m$ and $\varepsilon > 0$ be as in Theorem 3. There exists a positive number s_3, which is effectively computable in terms of ε, K and $\alpha_1, \ldots, \alpha_m$, with the property that for every integer $s \geq s_3$ there are a set $S = \{p_1, \ldots, p_s\}$ of rational prime numbers and a number α_0 with* (2.6), *such that*

$$g(\boldsymbol{\alpha}, S) \geq \exp\{(1-\varepsilon)n(c_K s)^{1/n}(\log s)^{(1/n)-1}\}.$$

Here $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_m)$.

It should be noted that both Theorems 3 and 4 with $m = 1$ imply the result of Moree and Stewart mentioned above.

The main tool in the proofs of Theorems 1-4 is a lower bound for the number of ideals in a given number field which have norm $\leq X$, are composed of prime ideals $\leq Y$, and which are composed of prime ideals outside a given finite set of prime ideals T. We have stated this result below since it is not in the literature and since it may have some independent interest. We first recall some history.

Let $\psi(X,Y)$ be the number of positive rational integers not exceeding X which are free of prime divisors larger than Y. Canfield, Erdős and Pomerance [5] proved that there exists an absolute constant C such that if X,Y are positive reals with $Y \geq 3$ and with $u := \frac{\log X}{\log Y} \geq 3$, then

$$(2.8)\quad \psi(X,Y) \;\geq\; X\exp\Big\{-u\big\{\log(u\log u)-1+ \\ +\frac{\log_2 u - 1}{\log u} + C\Big(\frac{\log_2 u}{\log u}\Big)^2\big\}\Big\}.$$

where $\log_2 u = \log\log u$. Further, Hildebrand [11] showed that for arbitrary fixed $\varepsilon > 0$, one has uniformly under the condition $X \geq 2$, $\exp\{(\log_2 X)^{\frac{5}{3}+\varepsilon}\} \leq Y \leq X$,

$$(2.9)\qquad \psi(X,Y) = X\rho(u)\Big\{1 + O\left(\frac{\log(u+1)}{\log Y}\right)\Big\},$$

where $\rho(u)$ denotes the Dickman-de Bruijn function.

More generally, let K be a number field. By an ideal of the ring of integers O_K we shall mean a non-zero ideal. Denote by $\psi_K(X,Y)$ the number of ideals of O_K with norm at most X composed of prime ideals of O_K of norm at most Y. Here the norm of an ideal $\mathfrak{a}$ is the cardinality of the residue class ring $O_K/\mathfrak{a}$. By Moree and Stewart [18, Theorem 2] there exists a constant $C_K > 0$, depending only on K, such that with X,Y and u as above we have

$$(2.10)\quad \psi_{K,T}(X,Y) \;\geq\; X\exp\Big\{-u\big\{\log(u\log u)-1+ \\ +\frac{\log_2 u - 1}{\log u} + C_K\Big(\frac{\log_2 u}{\log u}\Big)^2\big\}\Big\}.$$

This result has been proved by extending the method of Canfield, Erdős and Pomerance.

Now let T be a finite set of prime ideals of O_K, and denote by $\psi_{K,T}(X,Y)$ the number of ideals of O_K which have norm $\leq X$ and are composed of prime ideals which have norm $\leq Y$ and lie outside T. We prove the following:

THEOREM 5. *There exists a positive effectively computable number $C_{K,T}$ depending only on K and T such that for $X, Y \geq 1$ with $u := \frac{\log X}{\log Y} \geq 3$ we have*

$$\psi_{K,T}(X,Y) \geq X \exp\Big\{ -u\big\{ \log(u \log u) - 1 + \\ + \frac{\log_2 u - 1}{\log u} + C_{K,T}\Big(\frac{\log_2 u}{\log u}\Big)^2 \big\}\Big\}. \tag{2.11}$$

In the proof of Theorem 5 we did not use the ideas of Canfield, Erdős and Pomerance, but instead extended the arguments from Hildebrand's paper [11] mentioned above. Another more straightforward method to obtain a lower bound for $\psi_{K,T}$ such as (2.11) is by combining the estimate (2.10) for $\psi_K(X,Y)$ with an interval result for $\psi_K(X,Y)$ due to Moree [16]. Unfortunately, the result obtained by this approach is valid only for a much smaller X, Y-range, and it is not at all transparent whether the constant $C_{K,T}$ arising from this approach is effective. In [4] Buchmann and Hollinger, assuming the Generalized Riemann Hypothesis, established a non-trivial lower bound for $\psi_K(X,Y)$, uniform in K, involving the degree of the normal closure and the discriminant D_K of K. They did so by using the method of Canfield, Erdős and Pomerance. Our method to prove Theorem 5 can be used to obtain a variant of the result of Buchmann and Hollinger with much smaller error term. As a starting point in our approach one may take equation (11.RH) of Lang [14].

3 Proof of Theorem 5.

We recall some properties of the Dickman-de Bruijn function $\rho(u)$. This function is the unique continuous solution of the differential-difference equation $u\rho'(u) = -\rho(u-1)$ for $u > 1$ with initial condition $\rho(u) = 1$ in the interval $[0,1]$ (and, by convention, $\rho(u) := 0$ for $u < 0$). Recall that according to Hildebrand's estimate (2.9), $\rho(u)$ is the density of the set of integers $\leq X$ composed of prime numbers $\leq X^{1/u}$ as X tends to infinity; therefore, $0 \leq \rho(u) \leq 1$. In the following lemma we have collected some further easily provable properties of the Dickman-de Bruijn function that will be needed in the sequel.

LEMMA 1. *We have*
i) $u\rho(u) = \int_{u-1}^{u} \rho(t)dt$ for $u \geq 1$.
ii) $\rho(u) > 0$ *for* $u > 0$.
iii) $\rho(u)$ *is decreasing for* $u > 1$.
iv) $-\rho'(u)/\rho(u)$ *is increasing for* $u > 1$.
v) $-\rho'(u) \leq \rho(u)\log(2u\log^2(u+3))$ *for* $u > 0$, $u \neq 1$.
vi) $\rho(u-t) \leq \rho(u)4(2u\log^2(u+3))^t$ *for* $u \geq 0$ *and* $0 \leq t \leq 1$.

Proof. This is in essence [11, Lemma 6], see also [17, p. 30]. Parts v) and vi) are, however, modified so as to obtain explicit estimates valid for $u > 0$. They require some easy numerical verifications that are left to the interested reader. □

An important quantity in the study of the Dickman-de Bruijn function is the function $\xi(u)$. For any given $u > 1$, $\xi(u)$ is defined as the unique positive solution of the transcendental equation

$$\frac{e^{\xi}-1}{\xi} = u. \tag{3.1}$$

The quantity $\xi(u)$ exists and is unique, since $\lim_{x\downarrow 0}(e^x-1)/x = 1$ and since $(e^x-1)/x$ is strictly increasing for $x > 0$. The Fourier transform $\hat{\rho}$ of ρ involves the function $(e^s-1)/s$. By writing ρ as the Fourier transform of $\hat{\rho}$ and applying the saddle point method one obtains [22, p. 374] that for $u \geq 1$,

$$\rho(u) = \sqrt{\frac{\xi'(u)}{2\pi}} \exp\Big\{\gamma - \int_1^u \xi(t)dt\Big\}\{1 + O(\frac{1}{u})\}. \tag{3.2}$$

(It is not difficult to show that $\xi'(u) \sim 1/u$ as u tends to infinity.) For our purposes we need an effective lower bound of the quality of (3.2). The next lemma fulfils our needs.

LEMMA 2. *For* $u \geq 1$ *we have*

$$\exp\Big\{-\int_2^{u+1}\xi(t)dt\Big\} \leq \rho(u) \leq \exp\Big\{-\int_1^u \xi(t)dt\Big\}.$$

Proof. Let $f(u) = -\rho'(u)/\rho(u)$ denote the logarithmic derivative of $1/\rho(u)$. Using parts i) and iv) of Lemma 1 we deduce that

$$u = \int_{u-1}^{u}\frac{\rho(t)}{\rho(u)}dt = \int_{u-1}^{u} e^{\int_t^u f(s)ds}dt \leq \int_{u-1}^{u} e^{(u-t)f(u)}dt = \frac{e^{f(u)}-1}{f(u)},$$

and thus, by the monotonicity of $(e^x-1)/x$, that $f(u) \ge \xi(u)$ for $u>1$. By a similar argument we find that $f(u) \le \xi(u+1)$ for $u>0$ and $u \ne 1$. On noting that

$$\begin{aligned} \exp\Big(-\int_1^u \xi(s+1)ds\Big) &\le \rho(u) = \exp\Big(-\int_1^u f(s)ds\Big) \\ &\le \exp\Big(-\int_1^u \xi(s)ds\Big), \end{aligned}$$

the proof is completed. □

The method of bootstrapping allows one to obtain an asymptotic expression for $\xi(u)$ with error $O(\log^{-k} u)$ for arbitrarily large k. To illustrate this we do the first few iterations. From (3.1) we deduce that

$$\xi = \log\xi + \log u + O(\frac{1}{\xi\cdot u}), \quad \xi\cdot u \to \infty. \tag{3.3}$$

Notice that for u sufficiently large $1 < \xi < 2\log u$. It follows from (3.3) that $\xi = \log u + O(\log_2 u)$. Substituting this into the right-hand side of (3.3) then yields $\xi = \log u + \log_2 u + O(\log_2 u/\log u)$. Note that the implied constant is effective. By repeatedly substituting the lastly found asymptotic expression for $\xi(u)$ into the right-hand side of (3.3), one can calculate an asymptotic expression for $\xi(u)$ with error $O(\log^{-k} u)$ for arbitrary $k>1$, with effective implied constant. This then implies, using Lemma 2, that for arbitrary $k>1$ we can find an elementary explicit function $g_k(u)$ such that $\rho(u) \ge \exp(g_k(u) + O_k(u\log^{-k} u))$, where the implied constant is effective. For example, by substituting $\xi = \log u + \log_2 u + O(\log_2 u/\log u)$ into the right-hand side of (3.3) we obtain for $u \ge 3$,

$$\xi = \log u + \log_2 u + \frac{\log_2 u}{\log u} + O\Big((\frac{\log_2 u}{\log u})^2\Big).$$

Using Lemma 2 we then find that, for $u \ge 3$,

$$\rho(u) \ge \exp\Big\{-u\Big\{\log(u\log u) - 1 + \frac{\log_2 u - 1}{\log u} + O\Big((\frac{\log_2 u}{\log u})^2\Big)\Big\}\Big\}, \tag{3.4}$$

where the implied constant is effective.
Alternatively $g_k(u)$ can be computed using the convergent series expansion

$$\xi(u) = \log u + \log_2 u + \sum_{m=0}^{\infty}\sum_{k=1}^{\infty} c_{mk}\left(\frac{1}{\log u}\right)^m \left(\frac{1+u\log_2 u}{u\log u}\right)^k,$$

where the c_{mk} are explicitly computable real numbers, cf. [12]. (This formula corrects the one stated in [12] where there is a typo that, as Prof. Tenenbaum pointed out to us, was introduced by the printer after the proof-corrections had taken place.)

Now let K be an algebraic number field. We put $P(\mathfrak{a}) = \max\{N\mathfrak{p} \ : \ \mathfrak{p}|\mathfrak{a}\}$ for an ideal $\mathfrak{a} \neq (1)$ of O_K and $P((1)) = 1$ (here and in the sequel the symbol $\mathfrak{p}$ is exclusively used to indicate a prime ideal). We denote by $N_K(Y)$ the number of ideals of O_K of norm $\leq Y$ and for a given finite set of prime ideals T of O_K, by $N_{K,T}(Y)$ the number of ideals of O_K of norm $\leq Y$ which are coprime with each of the prime ideals from T. For instance from the arguments in Lang [15, Chap. VI-VIII] it follows that

$$N_K(Y) = A_K Y + O(Y^{1-1/[K:\mathbb{Q}]}), \quad \text{where } A_K = \mathrm{Res}_{s=1}\zeta_K(s)$$

is the residue of the Dedekind zeta-function at $s = 1$ (which as is well-known can be expressed in terms of invariants such as the class number and regulator of the field K) and where the implied constant is effective and depends only on K. By means of the principle of inclusion and exclusion it then follows that

$$\begin{aligned} N_{K,T}(Y) &= A_{K,T}Y + O(Y^{1-1/[K:\mathbb{Q}]}) \\ & \qquad \text{with } A_{K,T} = A_K \textstyle\prod_{\mathfrak{p}\in T}(1 - \frac{1}{N\mathfrak{p}}), \end{aligned} \tag{3.5}$$

where the implied constant is effective and depends only on K and T.

As before, we denote by $\psi_{K,T}(X,Y)$ the number of ideals of O_K of norm at most X which are composed of prime ideals which do not belong to the finite set of prime ideals T and, moreover, have norm at most Y. The ideals so counted form a free arithmetical semigroup satisfying the conditions of Theorem 1 of [17, Chapter 4]. It then follows that, for arbitrary fixed $\varepsilon \in (0,1)$, we have uniformly for $1 \leq u \leq (1-\varepsilon)\log_2 X/\log_3 X$ that

$$\psi_{K,T}(X,Y) \sim A_{K,T} X \rho(u) \quad \text{as } X \to \infty, \tag{3.6}$$

where $\log_3 X = \log\log\log X$. Thus we get a density interpretation of $\rho(u)$ similar to that for $\psi(X,Y)$.

The proof of (3.6) is based on the Buchstab functional equation for free arithmetical semigroups. In order to obtain Theorem 5, which gives a lower bound for $\psi_{K,T}(X,Y)$ valid for a much larger X,Y-region, a different functional equation will be used. This equation along with several other ideas that go into the proof of Theorem 5 are due to Hildebrand [11], cf. [22, pp.

388-389], who worked in the case where $K=\mathbb{Q}$ and T is the empty set. Put $\mathfrak{q}=\prod_{\mathfrak{p}\in T}\mathfrak{p}$. Define

$$\Lambda_{K,T}(\mathfrak{a})=\begin{cases}\log N\mathfrak{p} & \text{if } \mathfrak{a}=\mathfrak{p}^{m} \text{ for some } \mathfrak{p}\notin T \text{ and } m\geq 1,\\ 0 & \text{otherwise.}\end{cases}$$

Then for $X\geq Y$ we have

$$\begin{aligned}(3.7)\qquad &\psi_{K,T}(X,Y)\log X\\ &=\int_1^X \frac{\psi_{K,T}(t,Y)}{t}dt+\sum_{\substack{N\mathfrak{a}\leq X\\ P(\mathfrak{a})\leq Y}}\Lambda_{K,T}(\mathfrak{a})\cdot\psi_{K,T}(\tfrac{X}{N\mathfrak{a}},Y).\end{aligned}$$

In order to establish the validity of this equation we express the sum of all terms $\log N\mathfrak{a}$ with $\mathfrak{a}$ satisfying $N\mathfrak{a}\leq X$, $P(\mathfrak{a})\leq Y$ and $\mathfrak{a}$ coprime with $\mathfrak{q}$ in two different ways. On the one hand we find by integration by parts that this sum can be expressed as

$$\psi_{K,T}(X,Y)\log X-\int_1^X\frac{\psi_{K,T}(t,Y)}{t}dt,$$

on the other hand we notice that the sum can be rewritten as follows

$$\begin{aligned}\sum_{\substack{N\mathfrak{a}\leq X,\ \mathfrak{a}+\mathfrak{q}=(1)\\ P(\mathfrak{a})\leq Y}}\ \sum_{\mathfrak{b}|\mathfrak{a}}\Lambda_{K,T}(\mathfrak{b}) &= \sum_{\substack{N\mathfrak{b}\leq X\\ P(\mathfrak{b})\leq Y}}\Lambda_{K,T}(\mathfrak{b})\sum_{\substack{N\mathfrak{a}\leq X,\ \mathfrak{a}+\mathfrak{q}=(1)\\ \mathfrak{b}|\mathfrak{a},\ P(\mathfrak{a})\leq Y}}1\\ &= \sum_{\substack{N\mathfrak{b}\leq X\\ P(\mathfrak{b})\leq Y}}\Lambda_{K,T}(\mathfrak{b})\ \psi_{K,T}(\tfrac{X}{N\mathfrak{b}},Y),\end{aligned}$$

where we used that $\log N\mathfrak{a}=\sum_{\mathfrak{b}|\mathfrak{a}}\Lambda_{K,T}(\mathfrak{b})$ for any ideal $\mathfrak{a}$ coprime with $\mathfrak{q}$. Using functional equation (3.7) and Lemmata 3 and 4 below, we will deduce the crucial Lemma 5, and from that, Theorem 5.

Lemma 3. *Let K be a number field and T a finite set of prime ideals in O_K. Put $\log^+ Y=\max\{1,\log Y\}$. Then*

$$\sum_{N\mathfrak{a}\leq Y}\frac{\Lambda_{K,T}(\mathfrak{a})}{N\mathfrak{a}}=\log Y+c_{1,K,T}+E(Y)\quad \textit{for } Y\geq 1,$$

where $c_{1,K,T}$ is a constant depending on K and T and where for every $m\geq 1$ we have $|E(Y)|\leq c'_m(\log^+ Y)^{-m}$, with c'_m an effectively computable *constant depending on m, K and T.*

Proof. Let $\Pi_K(Y)$ denote the number of prime ideals of K of norm $\leq Y$. Theorems 1.3, 1.4 of Lagarias and Odlyzko [13] imply an effective version of the Prime Ideal Theorem of the shape $\Pi_K(Y) = Li(Y) + E_0(Y)$ where $Li(Y) = \int_2^Y (\log t)^{-1} dt$ and $|E_0(Y)| \leq c''_m Y(\log^+ Y)^{-m}$ for every $m \geq 2$, with c''_m an effectively computable constant depending on m and K. From this and the standard Stieltjes integration and partial summation arguments one obtains Lemma 3. □

LEMMA 4. *Let $0 < \theta \leq 1$, $m \geq 4$, $1 \leq u \leq Y^2$, $Y \geq e^{m^{3m}}$ and let c'_m be as in Lemma 3. Put*

$$S_\theta = \sum_{N\mathfrak{a} \leq Y^\theta} \frac{\Lambda_{K,T}(\mathfrak{a})}{N\mathfrak{a}} \cdot \rho(u - \tfrac{\log N\mathfrak{a}}{\log Y}).$$

Then

$$S_\theta = \log Y \int_0^\theta \rho(u-v)dv + E_1(\theta),$$

with

$$|E_1(\theta)| \leq 17 c'_m \rho(u) \Big\{ 2 + \frac{u \log^2(u+3)}{\log^{m-1} Y} \theta^{-m} \Big\}.$$

Proof. Using Lemma 3 we find by Stieltjes integration that

$$S_\theta = \int_0^\theta \rho(u-v) d\left(\sum_{N\mathfrak{a} \leq Y^v} \frac{\Lambda_{K,T}(\mathfrak{a})}{N\mathfrak{a}} \right) = \log Y \int_0^\theta \rho(u-v)dv + I_1(\theta) + I_2(\theta),$$

where $I_1(\theta) = E(Y^\theta)\rho(u-\theta) - E(1)\rho(u)$ and $I_2(\theta) = \int_0^\theta \rho'(u-v)E(Y^v)dv$. Using Lemma 1 vi) we deduce that

$$|I_1(\theta)| \leq c'_m \rho(u) \Big\{ 1 + \frac{8u \log^2(u+3)}{\log^m Y} \theta^{-m} \Big\}.$$

For notational convenience let us put $g(u) := \log(2u\log^2(u+3))$. Then using Lemma 1 v), vi) we obtain

$$|I_2(\theta)| \leq 4\rho(u)g(u) \Big\{ c'_m \int_0^{\log^{-1} Y} e^{vg(u)} dv + \int_{\log^{-1} Y}^\theta e^{vg(u)} |E(Y^v)| dv \Big\}.$$

The conditions on u and Y ensure that the first integral in the latter estimate is bounded above by $g(u)^{-1} \exp(g(u)/\log Y) \leq 8/g(u)$. We split up the integration range of the second integral at $\theta\log^{-1/m} Y$ and denote the corresponding integrals by $I_3(\theta)$ and $I_4(\theta)$, respectively. We have

$$|I_3(\theta)| \le c'_m \frac{e^{\theta g(u)\log^{-\frac{1}{m}} Y}}{\log^m Y}\int_{\log^{-1} Y}^{\theta\log^{-\frac{1}{m}} Y}\frac{dv}{v^m} \le \frac{c'_m}{\log Y}e^{\theta g(u)/\log^{\frac{1}{m}} Y} \tag{3.8}$$

and

$$|I_4(\theta)| \le \frac{c'_m\theta^{-m}}{\log^{m-1} Y}\int_{\theta\log^{-\frac{1}{m}} Y}^{\theta} e^{vg(u)}dv \le \frac{c'_m\theta^{-m}}{\log^{m-1} Y}\frac{2u\log^2(u+3)}{g(u)}. \tag{3.9}$$

Note that if $g(u)\le \log^{1/m} Y$, then $g(u)|I_3(\theta)|\le c'_m/4$. If $g(u) > \log^{1/m} Y$, then thanks to our assumption $Y \ge e^{m^{3m}}$, the right-hand side of (3.8) is smaller than the right-hand side of (3.9), therefore both $|I_3(\theta)|$ and $|I_4(\theta)|$ are bounded above by $\frac{c'_m\theta^{-m}}{\log^{m-1} Y}\frac{2u\log^2(u+3)}{g(u)}$. On adding the various estimates, our lemma follows. □

Lemma 5. *Let $m\ge 4$ be arbitrary and $1\le u\le Y^2$. Suppose that $Y\ge \max\{e^{m^{3m}}, e^{1500c'_m}\}$. Then*

$$\psi_{K,T}(X,Y) \ge X\rho(u)\Delta\exp\Big(-1224c'_m\Big\{\frac{\log(6(u+1))}{\log Y}+\frac{5\cdot 2^{m-1}(u+1)}{\log^{m-3} Y}\Big\}\Big),$$

where $\Delta := \inf_{Y\ge 1} N_{K,T}(Y)/Y$.

Proof. We set $\delta(u) := \inf_{0\le v\le u}\psi_{K,T}(Y^v, Y)/(Y^v\rho(v))$. Note that $\delta(u)\ge\Delta$ for $0\le u\le 1$. Let $u>1$. Functional equation (3.7) gives rise to the estimate

$$\begin{aligned}\psi_{K,T}(X,Y)\log X &\ge \sum_{N\mathfrak{a}\le Y}\Lambda_{K,T}(\mathfrak{a})\psi_{K,T}(\tfrac{X}{N\mathfrak{a}}, Y)\\ &\ge X\delta(u)S_{\frac{1}{2}} + X\delta(u-\tfrac{1}{2})(S_1 - S_{\frac{1}{2}}).\end{aligned}$$

By dividing this inequality by $X\rho(u)\log X = Xu\rho(u)\log Y$ and then using Lemma 4, Lemma 1 i) and the fact that δ is decreasing, we obtain

$$\frac{\psi_{K,T}(X,Y)}{X\rho(u)} \ge \delta(u)r(u) + \delta(u-\tfrac{1}{2})\{1 - r(u) - 2|E_1(\tfrac{1}{2})| - |E_1(1)|\},$$

where

$$r(u) = \frac{1}{u\rho(u)}\int_0^{\frac{1}{2}}\rho(u-v)dv\,.$$

Since by Lemma 1 iii), ρ is decreasing it follows that $r(u) \leq \frac{1}{2}$. Further,

$$2|E_1(\tfrac{1}{2})| + |E_1(1)| \leq f_m(u) := \frac{51c'_m}{\log Y}\Big\{\frac{2}{u} + \frac{5 \cdot 2^m}{\log^{m-3} Y}\Big\}.$$

Hence

$$\frac{\psi_{K,T}(X,Y)}{X\rho(u)} \geq \tfrac{1}{2}\delta(u) + (\tfrac{1}{2} - f_m(u))\delta(u - \tfrac{1}{2}). \tag{3.10}$$

We want to establish that

$$\delta(u) \geq \min(\Delta, \delta(u - \tfrac{1}{2}))e^{-6f_m(u-\frac{1}{2})}. \tag{3.11}$$

If $\delta(u) = \delta(u - \frac{1}{2})$, this inequality is trivially true. If $\delta(u) = \delta(1)$ the inequality is true as well, since $\delta(1) \geq \Delta$. So assume that $\delta(u) < \delta(u-\frac{1}{2})$ and $\delta(u) < \delta(1)$. Choose ε with $0 < \varepsilon < 1$. Then there exists $u' \in (\max(1, u - \frac{1}{2}), u]$ such that $\psi_{K,T}(X', Y)/(X'\rho(u')) \leq \delta(u)(1+\varepsilon)$, with $X' = Y^{u'}$. Using (3.10) with u' replacing u we then infer

$$\begin{aligned}\delta(u)(1+\varepsilon) &\geq \tfrac{1}{2}\delta(u') + (\tfrac{1}{2} - f_m(u'))\delta(u' - \tfrac{1}{2}) \\ &\geq \tfrac{1}{2}\delta(u) + (\tfrac{1}{2} - f_m(u - \tfrac{1}{2}))\delta(u - \tfrac{1}{2}).\end{aligned}$$

Since ε may be chosen arbitrarily small, the latter inequality implies that $\delta(u) \geq \delta(u-\frac{1}{2})(1-2f_m(u-\frac{1}{2}))$. The lower bound $Y \geq \exp(1500c'_m)$ ensures that $f_m(u - \frac{1}{2}) < 1/6$ and hence the validity of (3.11).

We now iterate (3.11), the last step being with an argument $u_0 > 1$ such that $\delta(u_0 - \frac{1}{2}) \geq \Delta$. Since f_m is decreasing, this yields $\delta(u) \geq \Delta \exp\{-6\sum_{k=0}^{2[u]} f_m(\frac{k+1}{2})\}$. Then Lemma 5 follows after an easy computation. $\square$

Proof of Theorem 5. By (3.5) (which is effective), there is an effective constant Δ_0 such that $\Delta \geq \Delta_0 > 0$. Now from this fact, Lemma 5 with $m = 6$ and (3.4) (where the implied constant can be made effective) we obtain (2.11) with some effective constant $C_{K,T} > 0$, provided that $1 \leq u \leq Y^2$ and $Y \geq Y_0$, where Y_0 is some effectively computable number depending on K and T. Note that if $u > Y^2$ and $Y \geq Y_1$ (with $Y_1 \geq Y_0$ effective and depending on K, T and $C_{K,T}$) then the right-hand side of (2.11) is < 1 so that (2.11) is trivially true (as $\psi_{K,T}(X,Y) \geq 1$). Further, if $Y \leq Y_1$ then for X exceeding some effectively computable number X_0 depending on K, T, Y_1 and $C_{K,T}$ we have again that the right-hand side of (2.11) is < 1, so that (2.11) holds. We can achieve that (2.11) holds for the remaining values for X, Y, i.e., $Y \leq Y_1$ and $X \leq X_0$, by enlarging the constant $C_{K,T}$ if necessary.

This completes the proof of Theorem 5. $\square$

Remark. Given any $k > 0$, a refinement of Theorem 5 with error term $\exp\{O(u \log^{-k} u)\}$ and effective implied constant can be given by carrying out the bootstrap process for $\xi(u)$ far enough.

4 Preparations for the proofs of Theorems 1–4.

We start with a simple result on polynomial equations.

LEMMA 6. *Let $Q \in \mathbb{C}[X_1, \ldots, X_m]$ be a non-trivial polynomial of total degree g. Let $A, B \in \mathbb{Z}$ with $A < B$. Then the set of vectors $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ with*

$$(4.1) \qquad Q(\mathbf{x}) = 0, \qquad A \le x_i \le B \text{ for } i = 1, \ldots, m$$

has cardinality at most $g \cdot (B - A + 1)^{m-1}$.

Proof. We proceed by induction on m. For $m = 1$ the lemma is obvious. Suppose $m > 1$. Assume the lemma holds true for polynomials in fewer than m variables. We may write

$$Q(X_1, \ldots, X_m) = \sum_{i=0}^{h} Q_i(X_1, \ldots, X_{m-1}) X_m^i$$

with $h \le g$, $Q_i \in \mathbb{C}[X_1, \ldots, X_{m-1}]$ of total degree $\le g - i$ for $i = 0, \ldots, h$ and with Q_h not identically zero. Let V be the set of tuples $\mathbf{x}$ with (4.1). Given $\mathbf{x} = (x_1, \ldots, x_m) \in V$ we write $\mathbf{x}' = (x_1, \ldots, x_{m-1})$.

First consider those $\mathbf{x} \in V$ for which $Q_h(\mathbf{x}') \neq 0$. There are at most $(B - A + 1)^{m-1}$ possibilities for $\mathbf{x}'$. Fix one of those $\mathbf{x}'$. Substituting x_i for X_i ($i = 1, \ldots, m-1$) in Q gives a non-zero polynomial of degree h in X_m. Hence for given $\mathbf{x}'$ there are at most h possibilities for x_m such that $Q(\mathbf{x}) = 0$. So altogether, there are at most $h(B - A + 1)^{m-1}$ vectors $\mathbf{x} \in V$ with $Q_h(\mathbf{x}') \neq 0$.

Now consider those $\mathbf{x} \in V$ for which $Q_h(\mathbf{x}') = 0$. Recall that Q_h has total degree at most $g - h$. So by the induction hypothesis, there are at most $(g - h)(B - A + 1)^{m-2}$ possibilities for $\mathbf{x}'$. For a fixed $\mathbf{x}'$, there are at most $B - A + 1$ possibilities for x_m. Therefore, there are at most $(g - h)(B - A + 1)^{m-1}$ vectors $\mathbf{x} \in V$ with $Q_h(\mathbf{x}') = 0$.

Combining this with the upper bound $h(B-A+1)^{m-1}$ for the number of vectors in V with $Q_h(\mathbf{x}') \neq 0$, we obtain that V has cardinality at most $g(B-A+1)^{m-1}$. This proves Lemma 6. $\square$

Let K be a number field. We denote by $\xi \mapsto \xi^{(i)}$ ($i = 1, \ldots, [K : \mathbb{Q}]$) the isomorphic embeddings of K into $\mathbb{C}$. The prime ideal decomposition of $\alpha \in O_K$ is by definition the prime ideal decomposition of the principal ideal (α) generated by α. We say that $\alpha \in O_K$ is coprime with the ideal $\mathfrak{a}$ if $(\alpha)+\mathfrak{a} = (1)$.

LEMMA 7. *Let $[K : \mathbb{Q}] = n$. Let $\mathfrak{a}$ be an ideal of O_K and let $\alpha \in O_K$ be coprime to $\mathfrak{a}$. Further, let T be the set of prime ideals dividing $\mathfrak{a}$. Then there are effectively computable constants $C_1, C_2, C_3 > 1$, depending only on $K, \mathfrak{a}$ such that for X, Y with $X > Y \geq C_1$, the number of non-zero $\xi \in O_K$ with*

$$(4.2) \qquad \begin{cases} |\xi^{(i)}| \leq C_2 X^{1/n} \text{ for } i = 1, \ldots, n, \\ \xi \equiv \alpha \pmod{\mathfrak{a}}, \\ (\xi) \text{ is composed of prime ideals of norm } \leq Y \end{cases}$$

is at least $C_3^{-1}\psi_{K,T}(X, Y)$.

Proof. Below, constants implied by $\ll$, $\gg$ depend only on K,$\mathfrak{a}$ and are all effective. For $\xi \in O_K$ let $||\xi||$ denote the maximum of the absolute values of the conjugates of ξ. Denote by h the class number of K. By the effective version of the Chebotarev density theorem from [13] (Theorems 1.3, 1.4) each ideal class of K contains a prime ideal outside T with norm bounded above effectively in terms of $K, \mathfrak{a}$. Let $\mathcal{H}$ consist of one such prime ideal from each ideal class.

Assume that Y exceeds the norms of the prime ideals from $\mathcal{H}$. Let $\mathfrak{b}$ be an ideal of norm at most X composed of prime ideals of norm at most Y lying outside T. Choose $\mathfrak{p}$ from $\mathcal{H}$ such that $\mathfrak{b} \cdot \mathfrak{p}$ is a principal ideal, (β), say. Then (β) has norm $\ll X$ and is composed of prime ideals of norm $\leq Y$ lying outside T. Further, there are at most h ways of obtaining a given principal ideal (β) by multiplying an ideal of norm at most X with a prime ideal from $\mathcal{H}$. Therefore, the number of principal ideals of norm $\ll X$, composed of prime ideals of norm at most Y and lying outside T, is at least $h^{-1}\psi_{K,T}(X, Y)$.

We choose from each residue class in $(O_K/\mathfrak{a})^*$ a representative γ for which $||\gamma||$ is minimal. Denote the set of these representatives by $\mathcal{R}$. Suppose $\mathcal{R}$ has cardinality m. Clearly, each element from $\mathcal{R}$ is composed of prime ideals outside T. Furthermore, of each element of $\mathcal{R}$ the absolute value of the norm can be bounded above effectively in terms of $K, \mathfrak{a}$.

Assume that Y exceeds the absolute values of the norms of the elements from $\mathcal{R}$. Then the elements of $\mathcal{R}$ are composed of prime ideals outside T of norm at most Y. Take a principal ideal (β) of norm $\ll X$ composed of prime ideals of norm at most Y lying outside T. According to, for instance, [21], Lemma A.15, there is a β' with $(\beta') = (\beta)$ and $||\beta'|| \ll X^{1/n}$. Clearly, β' is coprime with $\mathfrak{a}$, so there is a $\gamma \in \mathcal{R}$ with $\xi := \beta'\gamma \equiv \alpha \pmod{\mathfrak{a}}$. Note that $||\xi|| \ll X^{1/n}$, and that (ξ) is composed of prime ideals of norm at most Y lying outside T. There are at most m ways of getting a given element ξ with (4.2) by multiplying an element β' coprime with $\mathfrak{a}$ with an element from $\mathcal{R}$. In other words, there are at most m principal ideals of norm $\ll X$ composed of prime ideals of norm at most Y outside T which give rise to the same ξ with (4.2). Together with our lower bound $\psi_{K,T}(X,Y)/h$ for the number of principal ideals this implies that the number of ξ with (4.2) is at least $(hm)^{-1}\psi_{K,T}(X,Y)$. This proves Lemma 7. $\square$

For functions $f(y), g(y)$ we say that $f(y) = o(g(y))$ as $y \to \infty$ effectively in terms of parameters $z_1, \ldots, z_t$ if for every $\delta > 0$ there is an effectively computable constant y_0 depending on δ, $z_1, \ldots, z_t$ such that $|f(y)| \leq \delta |g(y)|$ for every $y \geq y_0$. Then we have:

Lemma 8. *Let $0 < \alpha < 1$. Further, let K be a number field and T a finite set of prime ideals of O_K. Then for $Y \to \infty$ there is an X such that*

$$\log X \leq \frac{2}{1-\alpha} Y^{1-\alpha}, \tag{4.3}$$

$$\frac{\psi_{K,T}(X,Y)}{X^{\alpha}} \geq \exp\Big\{\frac{1+o(1)}{1-\alpha} \cdot Y^{1-\alpha}(\log Y)^{-1}\Big\} \tag{4.4}$$

where the o-symbol is effective in terms of α, K, T.

Proof. Below all o-symbols are with respect to $Y \to \infty$ and effective in terms of α, K, T. Let $X = Y^u$ with $u \log u = Y^{1-\alpha}$. Thus,

$$u = (1+o(1))(1-\alpha)^{-1} Y^{1-\alpha}(\log Y)^{-1}$$

and

$$\log X = u \log Y = (1+o(1))(1-\alpha)^{-1} Y^{1-\alpha}.$$

Note that for Y sufficiently large, X satisfies (4.3). Further, $u \geq 3$. Now by our choice of u and by Theorem 5 we have

$$\begin{aligned}\frac{\psi_{K,T}(X,Y)}{X^\alpha} &\geq Y^{u(1-\alpha)} \exp\Big\{ -u\big(\log(u\log u) \ - 1 \ + o(1)\big)\Big\} \\ &\geq \exp\big((1+o(1))u\big) = \exp\big\{\tfrac{1+o(1)}{1-\alpha}\cdot Y^{1-\alpha}(\log Y)^{-1}\big\}\end{aligned}$$

which is (4.4). □

5 Proofs of Theorems 1 and 2.

Proof of Theorem 1. Constants implied by $\ll$ and $\gg$ are effective and depend only on $n, a_1, \ldots, a_n$ and the o-symbols are always with respect to $s \to \infty$ and effective in terms of $n, a_1, \ldots, a_n$. By "sufficiently large" we mean that the quantity under consideration exceeds some constant effectively computable in terms of $n, a_1, \ldots, a_n$. We denote the cardinality of a set A by $|A|$.

Let s be a positive integer and let ε be a positive real number. Put

$$\begin{aligned}&t = [(1-\varepsilon/2)s\,],\\ &Y = p_t,\ \ T = \{p_1, \ldots, p_t\}\end{aligned} \tag{5.1}$$

where p_i denotes the i-th prime. Note that, by an effective version of the Prime Number Theorem,

$$Y = (1+o(1))t\log t. \tag{5.2}$$

We choose X according to Lemma 8 with $\alpha = 1/n$, $K = \mathbb{Q}$, $T = \emptyset$.

Let $\varepsilon_i = \frac{a_i}{|a_i|}$ for $i = 1, \ldots, n$. The number of n-tuples $(x_1, \ldots, x_n)$ with each $\varepsilon_i x_i$ a positive integer of size at most X and composed of primes at most Y equals $\psi(X,Y)^n$. Since the sum $a_1x_1 + \cdots + a_nx_n$ is $\ll X$ and is a positive rational number with denominator $\ll 1$, there exists a positive rational $a_0 \ll X$ with denominator $\ll 1$ such that the set of tuples $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ with

$$\begin{cases} a_1x_1 + \cdots + a_nx_n = a_0 \\ 1 \leq \varepsilon_i x_i \leq X,\ x_i \text{ is composed of primes} \leq Y \text{ for } i = 1, \ldots, n, \end{cases} \tag{5.3}$$

has cardinality $\gg \psi(X,Y)^n/X$. Let R be the set of primes p dividing the numerator or denominator of a_0. By the (effective) Prime Number Theorem, $|R|$ is at most

$$(1+o(1))\log X/\log_2 X.$$

From (4.3) with $\alpha = 1/n$, (5.2), (5.1) we infer that $|R| = o(s)$ and then from (5.1) that $|R \cup T| < s$ provided s is sufficiently large. Let S be a set of primes of cardinality s containing $R \cup T$.

Clearly the numbers $\frac{x_i}{a_0}$ for $i = 1, \dots, n$ are S-units. Further, since $a_i(\frac{x_i}{a_0})$ is positive for $i = 1, \dots, n$, the subsums of $a_1x_1 + \cdots + a_nx_n$ are all non-zero. Thus equation (2.1) has $\gg \psi(X,Y)^n/X$ non-degenerate solutions in S-units. By (4.4) with $\alpha = 1/n$ and (5.2) we have for Y sufficiently large

$$\begin{aligned}\psi(X,Y)^n/X &\geq \exp\left((1+o(1))\tfrac{n^2}{n-1}Y^{1-(1/n)}(\log Y)^{-1}\right)\\ &\geq \exp\left((1+o(1))\tfrac{n^2}{n-1}t^{1-(1/n)}(\log t)^{-1/n}\right).\end{aligned}$$

Using (5.1) it follows at once that for s sufficiently large, equation (2.1) has more than $\exp\left((1-\varepsilon)\frac{n^2}{n-1}s^{1-(1/n)}(\log s)^{-1/n}\right)$ non-degenerate solutions in S-units. This proves Theorem 1. $\square$

Before proving Theorem 2 we observe that $g(\mathbf{a}, S)$ is the smallest integer g for which there exists a non-zero polynomial $P^* \in \mathbb{C}[X_1, \dots, X_{n-1}]$ of total degree g with

$$P^*(x_1, \dots, x_{n-1}) = 0 \quad \text{for every solution } (x_1, \dots, x_n) \text{ of (2.1).} \tag{5.4}$$

Indeed, let $P \in \mathbb{C}[X_1, \dots, X_n]$ be a polynomial of total degree $g(\mathbf{a}, S)$ with (2.2) which is not divisible by $a_1X_1 + \cdots + a_nX_n - 1$. Substituting $X_n = a_n^{-1}(1 - a_1X_1 - \cdots - a_{n-1}X_{n-1})$ in P we get a polynomial P^* which satisfies (5.4), has total degree at most $g(\mathbf{a}, S)$, and is not identically zero. On the other hand, any non-zero polynomial P^* with (5.4) must have total degree at least $g(\mathbf{a}, S)$ since it is not divisible by $a_1X_1 + \cdots + a_nX_n - 1$.

Proof of Theorem 2. Let $\varepsilon > 0$. By Theorem 1 with $n = 2$ we know that there is an effectively computable positive number t_1, which depends only on ε, such that for every integer $t \geq t_1$ there is a set of primes T of cardinality t for which the equation $x + y = 1$ in T-units x, y has at least

$$A(t) := \exp\left\{(4 - \tfrac{1}{2}\varepsilon)t^{1/2}(\log t)^{-1/2}\right\} \tag{5.5}$$

solutions. Fix such t and T. We first show by induction that for every $n \geq 2$ the n-tuple $\mathbf{1}_n = (1, \dots, 1)$ satisfies $g(\mathbf{1}_n, T) \geq A(t)$.

We are done for $n = 2$. Suppose $n \geq 3$, and that our assertion holds with $n-1$ in place of n. Thus $g(\mathbf{1}_{n-1}, T) \geq A(t)$. Let U be the set of tuples

$$(x_1, \dots, x_n) = (y_1, \dots, y_{n-2}, y_{n-1}z_1, y_{n-1}z_2) \tag{5.6}$$

where $(y_1, \ldots, y_{n-1})$ runs through the solutions of

$$y_1 + \cdots + y_{n-1} = 1 \quad \text{in } T\text{-units } y_1, \ldots, y_{n-1} \tag{5.7}$$

and where (z_1, z_2) runs through the solutions of

$$z_1 + z_2 = 1 \quad \text{in } T\text{-units } z_1, z_2. \tag{5.8}$$

Then from

$$y_1 + \cdots + y_{n-2} + y_{n-1}(z_1 + z_2) = 1$$

it follows that the tuples in U satisfy

$$x_1 + \cdots + x_n = 1. \tag{5.9}$$

Let $P \in \mathbb{C}[X_1, \ldots, X_{n-1}]$ be a non-zero polynomial of total degree $g(\mathbf{1}_n, T)$ such that $P(x_1, \ldots, x_{n-1}) = 0$ for every solution $(x_1, \ldots, x_n)$ in T-units of (5.9). Since the tuples in U consist of T-units, we have

$$P(y_1, \ldots, y_{n-2}, y_{n-1}z_1) = 0 \tag{5.10}$$

for every solution $(y_1, \ldots, y_{n-1})$ of (5.7) and every solution (z_1, z_2) of (5.8). Define the polynomial in $n-1$ variables

$$P^*(Y_1, \ldots, Y_{n-2}, Z_1) = P(Y_1, \ldots, Y_{n-2},\ Z_1 \cdot (1 - Y_1 - \cdots - Y_{n-2})). \tag{5.11}$$

Then P^* is not identically zero since P is not identically zero and since the change of variables

$$(X_1, \ldots, X_{n-1}) \mapsto (Y_1, \ldots, Y_{n-2},\ Z_1 \cdot (1 - Y_1 - \cdots - Y_{n-2}))$$

is invertible. Now from (5.10), (5.7) it follows that

$$P^*(y_1, \ldots, y_{n-2}, z_1) = 0 \tag{5.12}$$

for every solution $(y_1, \ldots, y_{n-1})$ of (5.7) and every solution (z_1, z_2) of (5.8). We distinguish two cases.

Case 1. There is a solution (z_1, z_2) of (5.8) such that the polynomial $P^*_{z_1}(Y_1, \ldots, Y_{n-2}) := P^*(Y_1, \ldots, Y_{n-2}, z_1)$ is not identically zero.

Then by (5.12), $P^*_{z_1}$ is a non-zero polynomial with $P^*_{z_1}(y_1, \ldots, y_{n-2}) = 0$ for every solution $(y_1, \ldots, y_{n-1})$ of (5.7). Hence $P^*_{z_1}$ has total degree $\geq g(\mathbf{1}_{n-1}, T) \geq A(t)$. Now by (5.11) this implies that the total degree $g(\mathbf{1}_n, T)$ of P is at least $A(t)$.

Case 2. For every solution (z_1, z_2) of (5.8), the polynomial $P^*_{z_1}(Y_1, \dots, Y_{n-2}) = P^*(Y_1, \dots, Y_{n-2}, z_1)$ is identically zero.

Then since (5.8) has at least $A(t)$ solutions, the polynomial P^* must have degree at least $A(t)$ in the variable Z_1. By (5.11) this implies that P has degree at least $A(t)$ in the variable X_{n-1}. So again we conclude that the total degree $g(\mathbf{1}_n, T)$ of P is at least $A(t)$. This completes our induction step.

Now let $\mathbf{a} = (a_1, \dots, a_n)$ be an arbitrary tuple of non-zero rational numbers and let R be the set of primes dividing the product of the numerators and denominators of $a_1, \dots, a_n$. Then $|R| \ll 1$.
Let s_1 be a positive number such that if s is an integer with $s \geq s_1$ then for

$$t := \left[\left(\tfrac{4-\varepsilon}{4-\varepsilon/2} \right)^2 \cdot s \right] + 1 \tag{5.13}$$

we have

$$t \geq t_1, \quad t + |R| < s.$$

Clearly, s_1 is effectively computable in terms of $n, a_1, \dots, a_n, \varepsilon$. Choose $s \geq s_1$ and let T be a set of t primes with $g(\mathbf{1}_n, T) \geq A(t)$. Choose any set of primes S of cardinality s containing $T \cup R$. Then since $a_1, \dots, a_n$ are S-units and by (5.5), (5.13) we have

$$g(\mathbf{a}, S) = g(\mathbf{1}_n, S) \geq g(\mathbf{1}_n, T) \geq A(t) \geq \exp\Big((4-\varepsilon) s^{1/2} (\log s)^{-1/2}\Big).$$

Theorem 2 follows. □

6 Proofs of Theorems 3 and 4.

We keep the notation from the previous sections. In particular, K is a number field of degree $n \geq 2$ and $\alpha_1, \dots, \alpha_m$ are $\mathbb{Q}$-linearly independent elements of O_K, where $1 \leq m \leq n-1$. Constants implied by $\ll$, $\gg$ are effectively computable in terms of K, $\alpha_1, \dots, \alpha_m$ and the o-symbols will be with respect to $s \to \infty$ and effective in terms of K, $\alpha_1, \dots, \alpha_n$. By "sufficiently large" we mean that the quantity under consideration exceeds some constant effectively computable in terms of $K, \alpha_1, \dots, \alpha_n$.

We order the rational primes p by the size of the smallest norm p^{k_p} of a prime ideal dividing (p). Let $p_1, \dots, p_s$ be the first s primes in this ordering and put $Y = p_s^{k_{p_s}}$. By the effective version of the Chebotarev density theorem from [13] (Theorems 1.3, 1.4) we have

$$Y = (1 + o(1)) c_K s \log s\,. \tag{6.1}$$

We have to make some further preparations. Choose $\gamma \in O_K$ with $\mathbb{Q}(\gamma) = K$; then the conjugates $\gamma^{(1)}, \ldots, \gamma^{(n)}$ are distinct. Further, choose $\delta \in O_K$ which is $\mathbb{Q}$-linearly independent of $\alpha_1, \ldots, \alpha_m$. Then there are indices $i_0, i_1, \ldots, i_m \in \{1, \ldots, n\}$ such that

$$\Delta := \begin{vmatrix} \alpha_1^{(i_0)} & \ldots & \alpha_m^{(i_0)} & \delta^{(i_0)} \\ \vdots & & \vdots & \vdots \\ \alpha_1^{(i_m)} & \ldots & \alpha_m^{(i_m)} & \delta^{(i_m)} \end{vmatrix} \neq 0.$$

Choose a rational prime number p such that p is coprime with γ and with the differences $\gamma^{(i)} - \gamma^{(j)}$ $(1 \leq i < j \leq n)$. Further, choose another rational prime number q such that q is coprime with δ and with Δ. Then by the Chinese Remainder Theorem, there is a $\beta \in O_K$ such that $\beta \equiv \gamma \pmod{p}$, $\beta \equiv \delta \pmod{q}$ and β is coprime with pq. It is clear that p, q, β can be determined effectively.

LEMMA 9. *For every $\xi \in O_K$ with $\xi \equiv \beta \pmod{pq}$ we have that $\mathbb{Q}(\xi) = K$ and that ξ is $\mathbb{Q}$-linearly independent of $\alpha_1, \ldots, \alpha_m$.*

Proof. Take $\xi \in O_K$ with $\xi \equiv \beta \pmod{pq}$. Then $\xi^{(i)} \equiv \beta^{(i)} \equiv \gamma^{(i)} \pmod{p}$ for $i = 1, \ldots, n$, so

$$\xi^{(i)} - \xi^{(j)} \equiv \gamma^{(i)} - \gamma^{(j)} \not\equiv 0 \pmod{p}$$

for $1 \leq i < j \leq n$, which implies that the conjugates of ξ are distinct. Hence $\mathbb{Q}(\xi) = K$. Likewise, we have $\xi^{(i)} \equiv \beta^{(i)} \equiv \delta^{(i)} \pmod{q}$ for $i = 1, \ldots, n$, so

$$\begin{vmatrix} \alpha_1^{(i_0)} & \ldots & \alpha_m^{(i_0)} & \xi^{(i_0)} \\ \vdots & & \vdots & \vdots \\ \alpha_1^{(i_m)} & \ldots & \alpha_m^{(i_m)} & \xi^{(i_m)} \end{vmatrix} \equiv \Delta \not\equiv 0 \pmod{q}.$$

Hence the determinant on the left-hand side is $\neq 0$, and therefore, ξ is $\mathbb{Q}$-linearly independent of $\alpha_1, \ldots, \alpha_m$. This proves Lemma 9. $\square$

Proof of Theorem 3. Let V be the $\mathbb{Q}$-vector space generated by $\alpha_1, \ldots, \alpha_m$. Choose an integral basis $\{\omega_1, \ldots, \omega_n\}$ of O_K such that $\omega_1, \ldots, \omega_m$ span V; this can be done effectively. Thus, every $\xi \in O_K$ can be expressed uniquely as $\xi = \sum_{j=1}^n x_j \omega_j$ with $x_j \in \mathbb{Z}$. By applying Cramer's rule to $\xi^{(i)} = \sum_{j=1}^n x_j \omega_j^{(i)}$ $(i = 1, \ldots, n)$ and using the fact that $\det(\omega_j^{(i)}) \neq 0$ we get

$$\max_{j=1,\ldots,n} |x_j| \ll \max_{i=1,\ldots,n} |\xi^{(i)}|.$$

We combine this with Lemma 7. Choose $X > Y$. Since by our construction, β is coprime with pq, it follows that the set of $\xi \in O_K$ with

$$\begin{aligned}
&\xi = \textstyle\sum_{j=1}^{n} x_j\omega_j, \quad x_j \in \mathbb{Z}, \quad |x_j| \ll X^{1/n} \text{ for } j = 1, \ldots, n, \\
&\xi \equiv \beta \pmod{pq}, \\
&(\xi) \text{ composed of prime ideals of norm} \le Y
\end{aligned}$$

has cardinality $\gg \psi_{K,T}(X, Y)$, where T is the set of prime ideals dividing (pq). Consequently, there is a number

$$\kappa = \sum_{j=m+1}^{n} y_j\omega_j \quad \text{with } y_j \in \mathbb{Z},\ |y_j| \ll X^{1/n} \text{ for } j = m+1, \ldots, n$$

such that the set of $\xi \in O_K$ with

$$(6.2) \qquad \begin{cases} \xi = \kappa + \sum_{j=1}^{m} x_j\omega_j, \quad x_j \in \mathbb{Z},\ |x_j| \ll X^{1/n} \text{ for } j = 1, \ldots, m, \\ \xi \equiv \beta \pmod{pq}, \\ (\xi) \text{ composed of prime ideals of norm} \le Y \end{cases}$$

has cardinality $\gg \psi_{K,T}(X, Y)/X^{1-(m/n)}$.

Pick ξ_0 satisfying (6.2). Then by Lemma 9, ξ_0 is an algebraic integer such that $\mathbb{Q}(\xi_0) = K$ and ξ_0 is $\mathbb{Q}$-linearly independent of $\alpha_1, \ldots, \alpha_m$. Since $\omega_1, \ldots, \omega_m$ span the same $\mathbb{Q}$-vector space as $\alpha_1, \ldots, \alpha_m$, there is a positive rational integer d such that the $\mathbb{Z}$-module generated by $d\omega_1, \ldots, d\omega_m$ is contained in the $\mathbb{Z}$-module generated by $\alpha_1, \ldots, \alpha_m$. Put $\alpha_0 := d\xi_0$; then α_0 satisfies (2.6).

We have $\xi_0 = \kappa + \sum_{j=1}^{m} y_j\omega_j$ with $y_j \in \mathbb{Z}$, $|y_j| \ll X^{1/n}$ for $j = 1, \ldots, m$. If for ξ as in (6.2) we write $x'_j = x_j - y_j$ $(j = 1, \ldots, m)$, we get

$$\xi = \xi_0 + \sum_{j=1}^{m} x'_j\omega_j \quad \text{with } x'_j \in \mathbb{Z},\ |x'_j| \ll X^{1/n} \text{ for } j = 1, \ldots, m$$

(where we have enlarged the constant implied by $\ll$). By expressing $d\omega_1, \ldots, d\omega_m$ as linear combinations of $\alpha_1, \ldots, \alpha_m$ with coefficients in $\mathbb{Z}$ we may express $d\xi$ with ξ satisfying (6.2) as

$$(6.3) \qquad d\xi = \alpha_0 + \sum_{j=1}^{m} x''_j\alpha_j \quad \text{with } x''_j \in \mathbb{Z},\ |x''_j| \ll X^{1/n} \text{ for } j = 1, \ldots, m$$

(again after enlarging the constant implied by $\ll$). Assuming, as we may, that d is composed of prime ideals of norm at most Y, we have for ξ with

(6.2) that $(d\xi)$ is composed of prime ideals of norm at most Y. Hence $|N_{K/\mathbb{Q}}(d\xi)|$ is composed of $p_1, \dots, p_s$. To simplify notation we write x_j instead of x_j''. Recalling that the set of elements with (6.2) has cardinality $\gg \psi_{K,T}(X,Y)/X^{1-(m/n)}$ and that $d\xi$ with ξ as in (6.2) can be expressed as (6.3), we obtain that the set of tuples $(x_1, \dots, x_m) \in \mathbb{Z}^m$ with

$$(6.4) \qquad \begin{cases} |N_{K/\mathbb{Q}}(\alpha_0 + x_1\alpha_1 + \cdots + x_m\alpha_m)| = p_1^{z_1} \cdots p_s^{z_s} \\ \qquad\qquad \text{for certain } z_1, \dots, z_s \in \mathbb{Z}, \\ |x_j| \ll X^{1/n} \text{ for } j = 1, \dots, m \end{cases}$$

has cardinality $\gg \psi_{K,T}(X,Y)/X^{1-(m/n)}$.

We have already observed that $Y \to \infty$ as $s \to \infty$. Further, from Lemma 8 with $\alpha = 1 - (m/n)$ and from (6.1) it follows that for arbitrarily large Y there is an X with

$$\begin{aligned} \psi_{K,T}(X,Y)/X^{1-(m/n)} &\geq \exp\left\{(1+o(1))\tfrac{n}{m} \cdot Y^{m/n}(\log Y)^{-1}\right\} \\ &\geq \exp\left\{(1+o(1))\tfrac{n}{m} \cdot (c_K s)^{m/n}(\log s)^{(m/n)-1}\right\}. \end{aligned}$$

Theorem 3 now follows directly. □

Proof of Theorem 4. In the proof of Theorem 3 we have shown that for every sufficiently large Y and every $X > Y$ there is an α_0 with (2.6), such that the set of tuples $\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m$ with (6.4) has cardinality $\gg \psi_{K,T}(X,Y)/X^{1-(m/n)}$.

Let $S = \{p_1, \dots, p_s\}$. Let $P \in \mathbb{C}[X_1, \dots, X_m]$ be a non-trivial polynomial of total degree $g = g(\boldsymbol{\alpha}, S)$ such that for each solution $(x_1, \dots, x_m, z_1, \dots, z_s)$ of (2.4) we have $P(x_1, \dots, x_m) = 0$. This implies in particular that $P(\mathbf{x}) = 0$ for each tuple $\mathbf{x}$ with (6.4). Now since the tuples $(x_1, \dots, x_m)$ with (6.4) have $|x_j| \ll X^{1/n}$ for $j = 1, \dots, m$, we have by Lemma 6 that the number of these tuples is $\ll g \cdot (X^{1/n})^{m-1}$. Together with our lower bound $\gg \psi_{K,T}(X,Y)/X^{1-(m/n)}$ for the number of tuples with (6.4), this gives

$$g \cdot X^{(m-1)/n} \gg \psi_{K,T}(X,Y)/X^{1-(m/n)}$$

or equivalently

$$g \gg \psi_{K,T}(X,Y)/X^{1-(1/n)}.$$

Again Y goes to infinity with s. Further, by Lemma 8 with $\alpha = 1 - (1/n)$ and (6.1) we have that for $Y \to \infty$ there is an X with

$$\begin{aligned} \psi_{K,T}(X,Y)/X^{1-(1/n)} &\geq \exp\left\{(1+o(1))n \cdot Y^{1/n}(\log Y)^{-1}\right\} \\ &\geq \exp\left\{(1+o(1))n \cdot (c_K s)^{1/n}(\log s)^{(1/n)-1}\right\}. \end{aligned}$$

This proves Theorem 4. $\Box$

Acknowledgement. We thank Prof. G. Tenenbaum for some helpful comments regarding Section 2.

References

[1] A. Bérczes, *Some new diophantine results on decomposable polynomial equations and irreducible polynomials*, Ph.D. thesis, Kossuth Lajos University, Debrecen, 2000.

[2] A. Bérczes, K. Győry, On the number of solutions of decomposable polynomial equations, *Acta Arith.* **101** (2002), 171-187.

[3] D. Berend, Y. Bilu, Polynomials with roots modulo every integer, *Proc. Amer. Math. Soc.* **124** (1996), 1663-1671.

[4] J.A. Buchmann, C.S. Hollinger, On smooth ideals in number fields, *J. Number Theory* **59** (1996), 82-87.

[5] E.R. Canfield, P. Erdős, C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", *J. Number Theory* **17** (1983), 1-28.

[6] P. Erdős, C.L. Stewart, R. Tijdeman, Some diophantine equations with many solutions, *Comp. Math.* **36** (1988), 37-56.

[7] J.-H. Evertse, On equations in S-units and the Thue-Mahler equation, *Invent. Math.* **75** (1984), 561-584.

[8] J.-H. Evertse, The number of solutions of decomposable form equations, *Invent. Math.* **122** (1995), 559-601.

[9] J.-H. Evertse, K. Győry, C.L. Stewart, R. Tijdeman, On S-unit equations in two unknowns, *Invent. Math.* **92** (1988), 461-477.

[10] A. Granville, personal communication.

[11] A. Hildebrand, On the number of positive integers $\leq x$ and free of prime factors $> y$, *J. Number Theory* **22** (1986), 289-307.

[12] A. Hildebrand, G. Tenenbaum, On a class of differential-difference equations arising in number theory, *J. Anal. Math.* **61** (1993), 145-179.

[13] J.C. Lagarias and A.M. Odlyzko, Effective versions of the Chebotarev density theorem, Algebraic Number Fields, A. Fröhlich ed., Academic Press (1977), 409-464.

[14] S. Lang, On the zeta functions of number fields, *Invent. Math.* **12** (1971), 337-345.

[15] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994.

[16] P. Moree, An interval result for the number field $\psi(x, y)$ function, *Manuscripta Math.* **76** (1992), 437-450.

[17] P. Moree, *Psixyology and Diophantine equations*, Ph.D. thesis, University of Leiden, 1993.
Available from http://web.inter.nl.net/hcc/J.Moree/.

[18] P. Moree, C.L. Stewart, Some Ramanujan-Nagell equations with many solutions, *Indag. Math. N.S.* **1** (1990), 465-472.

[19] H.P. Schlickewei, On norm form equations, *J. Number Theory* **9** (1977), 370-380.

[20] W.M. Schmidt, Linearformen mit algebraischen Koeffizienten II, *Math. Ann.* **191** (1971), 1-20.

[21] T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press, Cambridge, 1986.

[22] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics **46**, Cambridge University Press, Cambridge, 1995.

Adresses of the authors:

J.-H. Evertse and R. Tijdeman:
Universiteit Leiden, Mathematisch Instituut,
Postbus 9512, 2300 RA Leiden, The Netherlands
email evertse@math.leidenuniv.nl, tijdeman@math.leidenuniv.nl

P. Moree:
Universiteit van Amsterdam, KdV Instituut,
Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands
email moree@science.uva.nl

C.L. Stewart:
University of Waterloo, Department of Pure Mathematics,
Waterloo, Ontario, Canada, N2L 3G1
email cstewart@watserv1.uwaterloo.ca