Some Ramanujan–Nagell equations with many solutions

by P. Moree and C. L. Stewart

1 Introduction

Let $F(x,y)$ be a binary form with integer coefficients of degree $n \geq 3$ and let $S = \{p_1, \ldots, p_s\}$ be a set of prime numbers. In 1984 Evertse [5] proved that if the binary form F is divisible by at least three pairwise linearly independent linear forms in some algebraic number field then the number of solutions of

$$F(x,y) = p_1^{z_1} \cdots p_s^{z_s}, \tag{1}$$

in coprime integers x and y and integers $z_1, \ldots, z_s$ is at most

$$2 \times 7^{n^3(2s+3)}. \tag{2}$$

Equation (1) is known as a Thue-Mahler equation. Estimates for the number of solutions of (1) had been given earlier by Mahler [11] and Lewis and Mahler [10]. Recently Bombieri [1] proved that if F is of degree at least 6 and is without multiple factors then the number of solutions of (1) in coprime integers x and y and integers $z_1, \ldots, z_s$ is at most

$$(4(s+1))^2 (4n)^{26(s+1)}. \tag{3}$$

If we fix y as 1 in (1) we obtain a Ramanujan-Nagell equation. In [4] Erdös, Stewart and Tijdeman proved that the exponential dependence on s in estimates (2) and (3) is not far from the truth by giving examples of Ramanujan-Nagell equations with many solutions. Let ε be a positive number, let $2 = p_1, p_2, \ldots$ be the sequence of prime numbers and let n be an integer with $n \geq 2$. They proved that there exists a number s_0, which is effectively computable in terms of ε and n, such that if s is an integer with

$s \geq s_0$ then there exists a monic polynomial F of degree n with distinct roots and rational integer coefficients for which the equation

$$F(x) = p_1^{z_1} \cdots p_s^{z_s} \tag{4}$$

has at least

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

solutions in non-negative integers $x, z_1, \ldots, z_s$. The polynomials F constructed in [4], for which (4) has many solutions, have the special property that all their zeros are rational integers. The problem of proving a comparable result with F irreducible over the rationals was posed in [4]. The purpose of this paper is to establish such a result.

Theorem 1 *Let K be a field of degree n over $\mathbb{Q}$, ε be a positive number and $2 = p_1, p_2, \ldots$ be the sequence of prime numbers. There exists a number $s_0(\varepsilon, K)$, which depends on ε and K only, such that if s is an integer with $s \geq s_0(\varepsilon, K)$ then there exists an irreducible monic polynomial F in $\mathbb{Z}[x]$ of degree n and with a root in K for which the equation*

$$F(x) = p_1^{z_1} \cdots p_s^{z_s}, \tag{5}$$

has at least

$$\exp\{(n - \varepsilon)s^{1/n}/(\log s)^{1-1/n}\} \tag{6}$$

solutions in integers $x, z_1, \cdots, z_s$.

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 and 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 $F(x) \equiv 0 (\mathrm{mod} p)$ has a solution. It follows from the Chebotarev density theorem (see Theorems 1.3 and 1.4 of [8]) that

$$\pi_F(x) = C(K)(1 + o_K(1))\frac{x}{\log x}, \tag{7}$$

where $C(K)$ is a positive number which depends on K only. Further $1/n \leq C(K) \leq 1$ and if K is normal then $C(K) = 1/n$. On restricting the primes occurring on the right hand side of (4) to those primes p for which there is a solution of $F(x) \equiv 0 (\mathrm{mod} p)$, and appealing to (7) we obtain the following corollary of Theorem 1.

Corollary *Let K be a field of degree n over $\mathbb{Q}$ and let ε be a positive number. There exists a number $s_1(\varepsilon, K)$, which depends on ε and K only, such that if s is an integer with $s \geq s_1(\varepsilon, K)$ then there exists an irreducible monic polynomial F in $\mathbb{Z}[x]$ of degree n and with a root in K and there exist primes $q_1, \ldots, q_s$ for which the equation*

$$F(x) = q_1^{z_1} \cdots q_s^{z_s} \tag{8}$$

has at least

$$\exp\{(C(K))^{-1/n}(n-\varepsilon)s^{1/n}/(\log s)^{1-1/n}\} \tag{9}$$

solutions in integers $x, z_1, \ldots, z_s$.

In order to prove Theorem 1 we require an estimate from below for $\psi_K(x, y)$, the number of ideals in the ring of algebraic integers of K with norm at most x all of whose prime ideal divisors have norm at most y. Let $\log_2 x$ denote $\log\log x$. For the proof of Theorem 1 we shall appeal to the following result.

Theorem 2 *Let K be a field of finite degree over $\mathbb{Q}$. There exists a positive number $C_1 = C_1(K)$, which depends upon K, such that for all $x \geq 1$ and $u \geq 3$,*

$$\psi_K(x, x^{1/u}) \geq x \exp\left\{-u\left(\log u + \log_2 u - 1 + \frac{\log_2 u - 1}{\log u} + C_1\left(\frac{\log_2 u}{\log u}\right)^2\right)\right\}.$$

Canfield, Erdös and Pomerance [3] proved this result in the case that $K = \mathbb{Q}$. We shall show that Theorem 2 follows from straightforward generalization of their argument.

The Dickman-de Bruijn function $\rho(u)$ is a positive, continuous, non-increasing function on $[0, \infty)$ defined recursively by

$$\rho(u) = 1 \quad \text{for} \quad 0 \leq u \leq 1,$$

and, for $N = 1, 2, \ldots$,

$$\rho(u) = \rho(N) - \int_N^u v^{-1}\rho(v-1)dv \quad \text{for} \quad N < u \leq N+1.$$

In 1951 de Bruijn [2] proved that for $u \geq 3$,

(10)

$$\rho(u) = \exp\left\{-u\left(\log u + \log_2 u - 1 + \frac{\log_2 u - 1}{\log u} + O\left(\left(\frac{\log_2 u}{\log u}\right)^2\right)\right)\right\}.$$

U. Krause [12] has recently proved, apparently by generalizing Theorem 2 of [7], that for $x \geq 1, u \geq 1$ and $\varepsilon > 0$,

$$\log\left(\frac{\psi_K(x, x^{1/u})}{x}\right) \geq \log\rho(u) + O_{K,\varepsilon}(u\exp(-c\ (\log u)^{3/5-\varepsilon})),$$

for c a positive constant. Combined with (10) this will give an alternative proof of Theorem 2.

We remark that for the proof of Theorem 1 we do not require the full strength of Theorem 2. The weaker estimate

$$\psi_K(x, x^{1/u}) \geq x\exp\{-u(\log u + \log_2 u - 1 + o_K(1))\}$$

would suffice.

2 Proof of Theorem 2

Let K be a finite extension of $\mathbb{Q}$ with ring of algebraic integers O_K. For each ideal a in O_K let $N\mathsf{a}$ denote the norm of a. Let $\pi_K(x)$ denote the number of prime ideals p of O_K with $N\mathsf{p}$ at most x. By Landau's Primidealsatz [9, Satz 191], for $x \geq 2$,

$$\pi_K(x) = \text{li}\ x + O_K(x\exp(-c_1(\log x)^{1/2})), \tag{11}$$

where c_1 is a positive number which depends on K only. Further, it follows from (11) by Abel summation that for $x \geq 3$,

$$\sum_{N\mathsf{p}\leq x}\frac{1}{N\mathsf{p}} = \log_2 x + c_2 + O_K(\exp(-c_1(\log x)^{1/2})) \tag{12}$$

where c_2 is a number which depends on K only.

In [6, 1.14] Hazlewood gave the following estimate for $\psi_K(x, x^{1/u})$.

Lemma 1 *For* $2 < u \le (\log x)^{1/3}$

$$\psi_K(x, x^{1/u}) = c_3 x\rho(u) + O_K(xu^2\rho(u)/\log x),$$

where c_3 *is a positive number which depends on* K *only.*

Following Canfield, Erdös and Pomerance we first establish a crude lower bound for $\psi_K(x, x^{1/u})$.

Lemma 2 *There is a number* c_4*, which depends on* K*, such that if* $u \ge c_4$ *and* $x \ge 1$ *then*

$$\psi_K(x, x^{1/u}) > x/u^{4u}. \tag{13}$$

Proof Since $\psi_K(x, x^{1/u}) \ge 1$ the result is trivial if $u^{4u} > x$ and so we may assume that $x \ge u^{4u}$. Thus, by Lemma 1 and (10), (13) holds provided that u is at most $(\log x)^{1/3}$ and u is sufficiently large. Therefore we may suppose that $u > (\log x)^{1/3}$.

Put $\pi'_K(x) = \max\{1, \pi_K(x)\}, \log^+ x = \max\{1, \log x\}$ and

$$\gamma = \inf_{x \ge 1} \pi'_K(x)/(x/\log^+ x).$$

Note that $\gamma > 0$, by (11). Now put $m = [u]$ and $\vartheta = u - [u]$. We have

$$\psi_K(x, x^{1/u}) \ge \frac{(\pi'_K(x^{1/u}))^m \pi'_K(x^{\vartheta/u})}{(m+1)!}$$

$$\ge \left(\frac{\gamma x^{1/u}}{\log^+(x^{1/u})}\right)^m \left(\frac{\gamma x^{\vartheta/u}}{\log^+(x^{\vartheta/u})}\right)((m+1)!)^{-1}.$$

Thus for u sufficiently large,

$$\psi_K(x, x^{1/u}) \ge \left(\frac{\gamma u x^{1/u}}{\log x}\right)^m \left(\frac{\gamma x^{\vartheta/u}}{\log x}\right) u^{-m}$$

$$\ge x \exp\{-(u+1)(\log_2 x - \log \gamma)\}.$$

Since $3 \log u > \log_2 x$ the result follows.

Proof of Theorem 2 The proof of Theorem 2 is very similar to the proof of Theorem 3.1 of [3]. We shall now indicate the modifications to the proof of Theorem 3.1 of [3] which are required to transform it to a proof of Theorem 2.

We replace $\psi(x,y)$ by $\psi_K(x,y)$ and $D(u)$ by $D_K(u)$ where

$$D_K(u) = \inf_{x \ge 1} \ \frac{1}{x}\ \psi_K(x, x^{1/u}).$$

Next let $m_{j,1}, m_{j,2}, \ldots$, now denote the norms of the different ideals composed of exactly $[\alpha_j u]$, not necessarily distinct, prime ideals with norms in I_j. Notice that in contrast to the case $K = \mathbb{Q}$ some $m_{j,k}'s$ might be equal. Let $m_1, m_2, \ldots$ denote the integers of the form $m_{1,i_1}, m_{2,i_2}, \ldots, m_{k,i_k}$; here again same values might occur repeatedly. In place of (3.5) of [3] we have the fundamental inequality

$$\psi_K(x, x^{1/u}) \ge \sum_i \psi_K(x/m_i, w), \quad w = x^{(1/u)(1-(k/(\log u)^3))}.$$

Further in place of $\sum_{p \in I_j} 1/p$ in expressions (3.11) and (3.12) of [3] we put $\sum_{N\mathfrak{p} \in I_j} 1/N\mathfrak{p}$ and to establish the analogue of (3.12) we appeal to (12). Note also that the constants implied by the symbols O may now depend on K. With these changes all inequalities and formulae up to and including (3.15) of [3] remain valid. We now appeal to Lemma 2 and (3.9) to deduce that for large u

$$\log D_K(v) \ge -4v \log v \ge -4u.$$

This replaces the estimates $\log D(v) \ge -3u$ but this change does not affect the subsequent argument and the result follows as in [3].

3 Proof of Theorem 1

Throughout this section let K be an algebraic number field with $[K : \mathbb{Q}] = n$ and let $N(\ \ )$ denote the norm from K to $\mathbb{Q}$. We shall assume $n > 1$ since Theorem 1 plainly holds when $n = 1$. We define the function $g_K(y)$ for y in $\mathbb{R}$ by

$$g_K(y) = \max_{x \ge 1} \frac{\psi_K(x,y)}{x^{1-1/n}}.$$

Observe that $g_K(y)$ is well defined since

$$\psi_K(x,y) \le \prod_{N\mathfrak{p} \le y} \left(\frac{\log x}{\log N\mathfrak{p}} + 1 \right).$$

Lemma 3 *Let $\varepsilon > 0$. There is a number c_5 which depends on K and ε such that if $y \geq c_5$ then*

$$g_K(y) \geq \exp\{(n-\varepsilon)y^{1/n}/\log y\}.$$

Proof Put $x_1 = \exp(ny^{1/n})$ and $u = ny^{1/n}/\log y$. Then certainly

$$g_K(y) \geq \frac{\psi_K(x_1, y)}{x_1^{1-1/n}}. \tag{14}$$

Further,

$$\log u = \log n + \frac{\log y}{n} - \log_2 y \tag{15}$$

and

$$\log_2 u = \log_2 y - \log n + o(1). \tag{16}$$

Thus, by Theorem 2, (15) and (16),

$$\psi_K(x_1, y) \geq \exp\left\{ny^{1/n} - \frac{ny^{1/n}}{\log y}\left(\frac{\log y}{n} - 1 + o_K(1)\right)\right\}.$$

Therefore, by (14),

$$g_K(y) \geq \exp\left\{\left(\frac{ny^{1/n}}{\log y}\right)(1 + o_K(1))\right\},$$

and the lemma follows.

Let x and c be positive real numbers with $x \geq 1$. We define $V(x,c)$ by

$$V(x,c) = \{\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n \mid |v_i| \leq cx^{1/n} \text{ for } i = 1, \ldots, n\}.$$

Lemma 4 *Let $\{1, \alpha_2, \ldots, \alpha_n\}$ be an integral basis for O_K. Let A be a subset of $V(x,c)$. The number of pairs $(\mathbf{u}, \mathbf{v})$ with $\mathbf{u} = (u_1, 0, \ldots, 0) \in V(x,c)$ and $\mathbf{v} \in A$ such that $\mathbb{Q}(u_1 - (v_1 + v_2\alpha_2 + \cdots + v_n\alpha_n)) = K$ is at least*

$$(2[cx^{1/n}] + 1)|A| - c_0 x^{1/2+1/n},$$

where c_0 is computable in terms of c and K.

Proof Let c_6, c_7, c_8 denote positive numbers which depend on c and K. The number of pairs $(\mathbf{u}, \mathbf{v})$ with $\mathbf{u} = (u_1, 0, \ldots, 0) \in V(x, c)$ and $\mathbf{v} \in A$ is $(2[cx^{1/n}] + 1)|A|$. Thus it suffices to show that there are at most $c_6 x^{1/2}$ elements $\mathbf{v} \in V(x, c)$ with $\mathbb{Q}(v_1 + v_2\alpha_2 + \cdots + v_n\alpha_n) \neq K$.

There are at most c_7 proper subfields of K and each is of degree at most $n/2$. Suppose that K' is a proper subfield of K of degree m over $\mathbb{Q}$ and that $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is an integral basis for $O_{K'}$. We may express the elements of this basis in terms of the integral basis $\{1, \alpha_2, \ldots, \alpha_n\}$ to get

$$\beta_i = b_{1,i} + b_{2,i}\alpha_2 + \cdots + b_{n,i}\alpha_n, \quad \text{for} \quad i = 1, \ldots, m.$$

The vectors $(b_{1,i}, \ldots, b_{n,i})$ for $i = 1, \ldots, m$ generate a sublattice of $V(x, c)$ with at most $c_8 x^{m/n}$ points. Since $m \leq n/2$ and there are at most c_7 such subfields the result follows.

Proof of Theorem 1 Let $c_9, c_{10}, \ldots$ be numbers which are computable in terms of K. Let $\sigma_1, \ldots, \sigma_n$ denote the $\mathbb{Q}$-isomorphisms of K into $\mathbb{C}$ and for any $\vartheta \in K$ put $\sigma_i(\vartheta) = \vartheta^{(i)}$ for $i = 1, \ldots, n$. Let $1, \alpha_2, \ldots, \alpha_n$ be an integral basis for O_K for which

$$\max\{|\alpha_j^{(i)}| \mid 1 \leq j \leq n, 1 \leq i \leq n\}$$

is minimal. Thus

$$\max_{i,j} |\alpha_j^{(i)}| < c_9.$$

Let h be the class number of K and let H be a set of ideals of O_K with exactly one ideal from each ideal class of the ideal class group. Choose the ideals in H to have minimal norm. Then the norm of an ideal from H is at most c_{10}. Next let x and y be real numbers with $x \geq y \geq c_{10}$. For each ideal a of O_K we denote the greatest norm of a prime ideal divisor of a by $P\mathsf{a}$ with the convention that $P(0) = P(1) = 1$. To each ideal a of O_K of norm at most x with $P\mathsf{a} \leq y$ we associate the principal ideal (α) obtained by multiplying a by the appropriate member of H. Then $N(\alpha) \leq c_{10}x$ and $P(\alpha) \leq y$. Further, every principal ideal (δ) with $N(\delta) \leq c_{10}x$ and $P(\delta) \leq y$ occurs in this manner at most h times. Thus the number of principal ideals in O_K of norm at most $c_{10}x$ and free of prime ideal divisors of norm greater than y is at least $\psi_K(x, y)/h$.

For each principal ideal a in O_K there is a γ in O_K with $\mathsf{a} = (\gamma)$ and such that

$$|\gamma^{(i)}| \leq c_{11} N(\gamma)^{1/n}, \quad \text{for} \quad i = 1, \ldots, n,$$

see for example Lemma A.15 of [13]. Thus there are at least $\psi_K(x, y)/h$ numbers γ in O_K such that

$$|\gamma^{(i)}| \leq c_{11}(c_{10}x)^{1/n}, \quad \text{for} \quad i = 1, \ldots, n,$$

with $N(\gamma) \leq c_{10}x$ and $P(\gamma) \leq y$. We now express these numbers γ in terms of the integral basis $\{1, \alpha_2, \ldots, \alpha_n\}$ of O_K. We have

$$\gamma^{(i)} = v_1 + v_2\alpha_2^{(i)} + \cdots + v_n\alpha_n^{(i)},$$

for $i = 1, \ldots, n$ with $v_i \in \mathbb{Z}$ for $i = 1, \ldots, n$. By Cramer's rule

$$|v_i| < c_{12}x^{1/n}, \quad \text{for} \quad i = 1, \ldots, n.$$

Let $A = A(x, y, c_{12})$ be the set of elements $\mathbf{v} = (v_1, \ldots, v_n) \in V(x, c_{12})$ for which $N(v_1 + v_2\alpha_2 + \cdots + v_n\alpha_n)$ does not contain prime divisors larger than y. Then $|A| \geq \psi_K(x, y)/h$. Thus by Lemma 4 the number of pairs $(\mathbf{u}, \mathbf{v})$ with $\mathbf{u} = (u_1, 0, \ldots, 0) \in V(x, c_{12})$ and $\mathbf{v} \in A$ for which $\mathbb{Q}(u_1 - (v_1 + v_2\alpha_2 + \cdots + v_n\alpha_n)) = K$ is at least

$$(2[c_{12}x^{1/n}] + 1)\psi_K(x, y)/h - c_{13}x^{1/2+1/n}$$

and the number of differences $\mathbf{u} - \mathbf{v}$ with $\mathbf{u}, \mathbf{v}$ as above is at most

$$(4c_{12}x^{1/n} + 1)(2c_{12}x^{1/n} + 1)^{n-1} \leq c_{14}x.$$

Thus there is a difference $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{Z}^n$ for which $\mathbb{Q}(d_1 + d_2\alpha_2 + \cdots + d_n\alpha_n) = K$ and for which there are at least

$$c_{15}\frac{\psi_K(x, y)}{x^{1-1/n}} - c_{16} \tag{17}$$

solutions of the equation $\mathbf{u} - \mathbf{v} = \mathbf{d}$ with $\mathbf{u} = (u_1, 0, \ldots, 0) \in V(x, c_{12})$ and $\mathbf{v} \in A$. We now take $y = p_s$ and choose x so that $\psi_K(x, y)/x^{1-1/n}$ is maximized. Let $\varepsilon > 0$. Then by the prime number theorem $p_s \sim s \log s$ and so by (17) and Lemma 3 there exists a number $s_0(\varepsilon, K)$, which depends on ε and K, such that for each s with $s > s_0(\varepsilon, K)$ there is a $\mathbf{d} \in \mathbb{Z}$ with $\mathbb{Q}(d_1 + d_2\alpha_2 + \cdots + d_n\alpha_n) = K$ and for which the equation

$$\mathbf{u} - \mathbf{v} = \mathbf{d}, \tag{18}$$

with $\mathbf{u} = (u_1, 0, \ldots, 0) \in V(x, c_{12})$ and $\mathbf{v} \in A(x, p_s, c_{12})$, has at least

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

solutions. For each $s > s_0(\varepsilon, K)$ we define $F(= F_s)$ in $\mathbb{Z}[z]$ by $F(z) = N(z - (d_1 + d_2\alpha_2 + \cdots + d_n\alpha_n))$. Note that F is monic, irreducible of degree n and has a root in K. Further for each solution $(\mathbf{u}, \mathbf{v})$ of (18), $z = u_1$ yields a solution of (5) since $N(v_1 + v_2\alpha_2 + \cdots + v_n\alpha_n)$ does not contain prime factors larger than y, and the result follows.

Acknowledgement Part of this work is derived from the first author's M.Sc. thesis, written under the direction of Professor R. Tijdeman. He wishes to thank him for his inspiration and encouragement.

References

[1] Bombieri, E., On the Thue-Mahler equation. In: *Diophantine Approximation and Transcendence Theory* (Seminar, Bonn 1985), Wusthöltz, G. ed., Lecture Notes in Mathematics, **1290**, 213-243. Berlin, Heidelberg, New York: Springer Verlag, 1987.

[2] de Bruijn, N. G., The asymptotic behaviour of a function occurring in the theory of primes, *J. Indian Math. Soc.* (N. S.), **15**, 25-32 (1951).

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

[4] Erdös, P., Stewart, C. L. and Tijdeman, R., Some diophantine equations with many solutions, *Compos. Math.*, **66**, 37-56 (1988).

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

[6] Hazlewood, D. G., On ideals having only small prime factors, *Rocky Mountain J. of Math.*, **7**, 753-768 (1977).

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

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

[9] Landau, E., Einführung in die elementare und analytische Theorie der algebraischen Zahlen und Ideale, Teubner, Leipzig (1927); reprint Chelsea, New York (1949).

[10] Lewis, D. J. and Mahler, K., On the representation of integers by binary forms, *Acta Arith.*, **6**, 333-363 (1961).

[11] Mahler, K., Zur Approximation algebraischer Zahlen. II, Über die Anzahl der Darstellungen ganzer Zahlen durch Binärformen, *Math. Ann.*, **108**, 37-55 (1933).

[12] Schaal, W., Letter to R. Tijdeman (07-03-1989).

[13] Shorey, T. N. and Tijdeman, R., *Exponential Diophantine Equations*, Cambridge University Press, Cambridge (1986).

P. Moree
Department of Mathematics
and Computer Science
University of Leiden
2300 RA Leiden
The Netherlands

C. L. Stewart
Department of Pure Mathematics
Faculty of Mathematics
The University of Waterloo
Waterloo, Ontario
Canada N2L 3G1