Publ. Math. Debrecen
53 / 1-2 (1998), 225–233

On a generalization of the Ramanujan-Nagell equation

By B. BRINDZA (Debrecen)

Abstract. In the paper a new method is given to derive a reasonable upper bound for the number of solutions of the generalized Ramanujan-Nagell equation.

1. Introduction

There are several possibilities to generalize the classical diophantine equation $x^2+7=2^z$. For results related to the number of solutions of the equations

$$x^2+D=p^z, \quad p \nmid D,$$
$$x^2+D=p_1^{k_1}\cdot\ldots\cdot p_t^{k_t}, \quad p_i \nmid D,\ i=1,\ldots,t$$

we refer to [Be1], [Be2], [ML1], [ML2] and [E], respectively. Let $f(X)$ be a polynomial of degree n and b be a rational integer with $|b|>1$ and let M denote the Mahler height of f and s the number of distinct prime divisors of b. Then we have

Theorem. *If f has at least two distinct zeros and one of them is not rational then the equation*

(1) $$f(x)=b^z \text{ in } x,z\in\mathbb{Z},\ z>1$$

Mathematics Subject Classification: 11D41.
Key words and phrases: Diophantine equations, gap principle.
Research supported in part by Grant D23992 from the Hungarian National Foundation for Scientific Research.

has at most

$$2n^2(s+2)+6n^2(s+1)(ns+n+2)$$

solutions provided that $|b|>cM^{5n}$, *where* c *is an effectively computable constant depending only on* n.

Remarks. For a given z the equation (1) can be considered as a superelliptic equation, however, b is not necessarily bounded by a constant depending only on f since the tuple

$$\left\{\frac{z}{(z,r_1)},\dots,\frac{z}{(z,r_k)}\right\},$$

where $r_1,\dots,r_k$ are the multiplicities of the zeros of f may have special shapes like

$$(2,2,1,1,\dots,1) \quad \text{or} \quad (m,1,1,\dots,1)$$

(cf. [L], [B]) and then the equation (1) may possess infinitely many solutions. We point out that there is no assumption imposed on the g.c.d. of b and the semi-discriminant of f that is there seems to be no way to apply standard arguments (the bound for the number of solutions should not depend on the number of the distinct prime divisors of the semi-discriminant of f). In the special case when b is a prime the condition on the rationality of the zeros can be omitted. Indeed, if every zero of f is rational (b is prime) then a quite simple argument shows that (1) leads to the equation

$$Ap^u+Bp^v=C,$$

where A,B,C are non-zero integers uniquely determined by f. It has certainly at most one solution in positive integers (u,v).

2. Auxiliary results

Let $\mathbb{K}$ be an algebraic number field and let $d_{\mathbb{K}},r_{\mathbb{K}},D_{\mathbb{K}},R_{\mathbb{K}},h_{\mathbb{K}}$ denote the degree, the unit rank, the discriminant, the regulator and the ideal class number of $\mathbb{K}$, respectively. Denote by S a finite set of absolute values of $\mathbb{K}$ including all its archimedian (infinite) values; let q be its cardinality. Furhermore, let $\mathfrak{p}_1,\dots,\mathfrak{p}_t$ be the prime ideals of $\mathbb{K}$ corresponding to the nonarchimedian (finite) values of S.

Lemma 1. *There are S-units $\pi_1, \dots, \pi_{q-1}$ satisfying*

$$h(\pi_1)\cdots h(\pi_{q-1}) < \frac{((q-1)!)^2}{2^{q-2}d_{\mathbb{K}}^{q-1}} h_{\mathbb{K}} R_{\mathbb{K}} \prod_{i=1}^{t} \log N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_i),$$

where $h(\ )$ denotes the absolute logarithmic height and each $\gamma \in U_S$ can be written as a product

$$\gamma = \rho \pi_1^{k_1} \cdots \pi_{q-1}^{k_{q-1}}$$

with ρ a root of unity and

$$\max_{1\le i\le q-1} |k_i| \le \frac{((q-1)!)^3}{2^{q-2}} \left(\frac{6d_{\mathbb{K}}^3}{\log d_{\mathbb{K}}}\right)^{q-1} h(\gamma) h_{\mathbb{K}} R_{\mathbb{K}} \prod_{i=1}^{t} \log N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_i).$$

Proof. This is a consequence of Lemmas 1,3 in [B&Gy] and the proof of the main result of [B1].

Lemma 2. *Let α be a non-zero element in $\mathbb{K}$ with $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = N$. $\overline{|\alpha|}$ denotes the maximum of the absolute values of the conjugates of α. There exists a unit ϵ such that*

$$\overline{|\alpha\epsilon|} \le N^{\frac{1}{d_{\mathbb{K}}}} \exp\left\{\left(\frac{6r_{\mathbb{K}}d_{\mathbb{K}}^2}{\log d_{\mathbb{K}}}\right)^{r_{\mathbb{K}}} \frac{r_{\mathbb{K}}}{2} R_{\mathbb{K}}\right\}.$$

Proof. See [Gy, Lemma 3].

Lemma 3. *Let α be a zero of the polynomial $f(X)$ and set $\mathbb{K} = \mathbb{Q}(\alpha)$. Then*

$$|D_{\mathbb{K}}| \le n^n M^{2n-2},\ h_{\mathbb{K}} R_{\mathbb{K}} < n^{4n} M^{2(n-1)},\ 0.056 < R_{\mathbb{K}}.$$

Proof. See Mahler [M], Siegel [S] and Zimmert [Z], noting that $D_{\mathbb{K}}$ divides the discriminant of $f(X)$.

Lemma 4. *If f has at least two distinct zeros then all the solutions to the equation* (1) *satisfy*

$$z < c_1 M^{3n},$$

where c_1 is an effectively computable constant depending only on n.

Proof. This result is a special case of the Theorem in [BBH].

Lemma 5 ([BPPW]). *Suppose that λ, $\eta_0, \dots, \eta_{t-1}$, μ, $\psi_0, \dots, \psi_{t-1}$ are nonzero complex numbers ($t \geq 1$) and that the equation*

$$\lambda \eta_0^{k_0} \cdots \eta_{t-1}^{k_{t-1}} + \mu \psi_0^{k_0} \cdots \psi_{t-1}^{k_{t-1}} = 1$$

has $t+2$ solutions $k_j = (k_{0,j}, \dots, k_{t-1,j}) \in \mathbb{Z}^t, j = 1, \dots t+2$. For compactness, write

$$K = \max_{0 \leq i \leq t-1, 1 \leq j \leq t+1} \{2, |k_{i,j+1} - k_{i,j}|\}.$$

and

$$\eta^{k_j} = \eta_0^{k_{0,j}} \cdots \eta_{t-1}^{k_{t-1,j}} \quad \text{and} \quad \psi^{k_j} = \psi_0^{k_{0,j}} \cdots \psi_{t-1}^{k_{t-1,j}}.$$

If

$$|\lambda \eta^{k_1}| \geq 6; \qquad |\eta^{k_{j+1}}/\eta^{k_j}| \geq 9(t+1)^{\frac{t}{2}} K^t, \ (j = 1, \dots, t+1)$$

then

$$\frac{1}{4}(t+1)^{\frac{t}{2}} K^t \geq |\lambda \eta^{k_1}|.$$

Remark. Actually, the proof is based upon Siegel's lemma or one can use Bombieri and Vaaler [B&V].

Proof. From the conditions we immediately have

$$\frac{1}{6} \geq |\lambda \eta^{k_1}|^{-1} > |\lambda \eta^{k_2}|^{-1} > \dots > |\lambda \eta^{k_{t+2}}|^{-1},$$

$$\left| \frac{\eta^{k_{j+1}}}{\eta^{k_j}} \right| \geq 9K^t \geq 18, \ j = 1, \dots, t+1,$$

$$\left| \frac{\psi^{k_j}}{\psi^{k_{j+1}}} \right| = \left| \frac{1 - \frac{1}{\lambda \eta^{k_j}}}{\eta^{k_{j+1} - k_j} - \frac{1}{\lambda \eta^{k_j}}} \right| \leq \frac{1 + \frac{1}{6}}{18 - \frac{1}{6}} < \frac{1}{15},$$

and

$$1 - \frac{1}{15} < \left| 1 - \frac{\psi^{k_j}}{\psi^{k_{j+1}}} \right| < 1 + \frac{1}{15}.$$

For $x \in \mathbb{C}$ with $|z| \leq \frac{1}{4}$ the simple inequality

$$\frac{5}{6}|z| \leq |\log(1 \pm z)| \leq \frac{7}{6}|z|$$

(log denotes the principal branch) and

$$1 - \eta^{k_{j+1}-k_j}/\psi^{k_{j+1}-k_j} = \lambda^{-1}\eta^{-k_j}(1 - \psi^{k_j - k_{j+1}})$$

imply

$$\frac{5}{6}\left(1 - \frac{1}{15}\right)|\lambda\eta^{k_j}|^{-1} \le |\log\left(1 - (1 - \eta^{k_{j+1}-k_j}/\psi^{k_{j+1}-k_j})\right)| \le \frac{7}{6}\left(1 + \frac{1}{15}\right)|\lambda\eta^{k_j}|^{-1}.$$

Hence there are rational integers $h_1, \dots, h_{t+1}$ for which

$$\frac{5}{6}\left(1 - \frac{1}{15}\right)|\lambda\eta^{k_j}|^{-1} \le \left|2\pi i h_j + \sum_{j=0}^{t-1}(k_{i,j+1} - k_{i,j})\log(\eta_i/\psi_i)\right| \le \frac{7}{6}\left(1 + \frac{1}{15}\right)|\lambda\eta^{k_j}|^{-1}.$$

From Siegel's lemma there exist rational integers $z_1, \dots, z_{t+1}$ not all zero, so that

$$\sum_{j=1}^{t+1} z_j(k_{i,j+1} - k_{i,j}) = 0; \quad i = 0, \dots, t-1$$

and

$$\max_{1\le j\le t+1}|z_j| \le (t+1)^{t/2}K^t.$$

Put

$$\Lambda_j = 2\pi i h_j + \sum_{i=0}^{t-1}(k_{i,j+1} - k_{i,j})\log(\eta_i/\psi_i), \quad j = 1, \dots, t+1,$$

$$Z = \max_{1\le j\le t+1}|z_j|, \quad K_1 = \frac{45}{8}(t+1)^{t/2}K^t.$$

Then $\Lambda_j \ne 0$ and

$$\sum_{j=1}^{t+1} z_j\Lambda_j = 2\pi i\sum_{j=1}^{t+1} z_j h_j,$$

furthermore,

$$\frac{|\Lambda_j|}{|\Lambda_{j+1}|} > \frac{\frac{5}{6}(1-\frac{1}{15})}{\frac{7}{6}(1+\frac{1}{15})}\left|\frac{\eta^{k_{j+1}}}{\eta^{k_j}}\right| = \frac{5}{8}\left|\frac{\eta^{k_{j+1}}}{\eta^{k_j}}\right| \geq K_1 > 15,$$

for $j = 1, \dots, t+1$. Let l be the smallest positive integer for which $z_l \neq 0$. Then

$$\begin{aligned}\Big|\sum_{j=1}^{t+1} z_j\Lambda_j\Big| &= \Big|\sum_{j=l}^{t+1} z_j\Lambda_j\Big| \geq |z_l||\Lambda_l| - Z\big(|\Lambda_{l+1}| + \ldots + |\Lambda_{t+1}|\big)\\ &\geq |\Lambda_l| - (t+1)^{\frac{t}{2}}K^t|\Lambda_l|\left(\frac{1}{K_1} + \frac{1}{K_1^2} + \ldots\right)\\ &= |\Lambda_l|\big(1 - (t+1)^{\frac{t}{2}}K^t(K_1-1)^{-1}\big) > 0,\end{aligned}$$

therefore,

$$\begin{aligned}2\pi \leq \Big|\sum_{j=l}^{t+1} z_j\Lambda_j\Big| &\leq Z\big(|\Lambda_{l+1}| + \ldots + |\Lambda_{t+1}|\big)\\ \leq Z|\Lambda_1|\left(\frac{1}{K_1} + \frac{1}{K_1^2} + \ldots\right) &\leq |\Lambda_1| - |\Lambda_1|\frac{Z}{1-\frac{1}{15}}\\ &\leq \frac{7}{6}\left(1+\frac{1}{15}\right)|\lambda\eta^{k_j}|^{-1}(t+1)^{\frac{t}{2}}K^t\frac{15}{14},\end{aligned}$$

which proves Lemma 4.

(The absolute constants certainly can be improved a bit, however it makes no difference in the proof of the Theorem).

3. Proof of the Theorem

Let $\alpha \notin \mathbb{Q}$ be a zero of f and write $\mathbb{K} = \mathbb{Q}(\alpha)$, moreover, let $\mathfrak{p}_1, \dots, \mathfrak{p}_l$ be the distinct prime ideal divisors of b in $\mathbb{K}$. Then we have $l \leq ns$. Let $\mathfrak{A}$ denote the denominator of the principal ideal generated by α (if any) and (x, z) be an arbitrary but fixed solution to (1). Then the ideal $\mathfrak{A}\langle x-\alpha\rangle_{\mathbb{K}}$ can be written as

$$\mathfrak{A}\langle x-\alpha\rangle_{\mathbb{K}} = \mathfrak{p}_1^{r_1} \cdot \ldots \cdot \mathfrak{p}_l^{r_l}.$$

In the sequel, $c_1, c_2, \dots$ will denote effectively computable constants depending only on n. Let τ be a generator of $\mathfrak{A}^{h_{\mathbb{K}}}$ with

$$\overline{|\tau|} < N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{A})^{\frac{h_{\mathbb{K}}}{n}} \exp\left\{ \left(\frac{6r_{\mathbb{K}} d_{\mathbb{K}}^2}{\log d_{\mathbb{K}}} \right)^{r_{\mathbb{K}}} \frac{r_{\mathbb{K}}}{2} R_{\mathbb{K}} \right\},$$

noting that $\mathfrak{A}$ divides the leading coefficients of f, therefore $|N(\mathfrak{A})| \leq M^n$. The element $\tau(x-\alpha)^{h_{\mathbb{K}}}$ can be considered as an S-unit, and the unit-group is determined by the prime ideal divisors of b and the rank r_1 of it is bounded by $ns + n - 1$.

Let $\pi_1, \dots, \pi_{r_1}$ be a generating set of this group with

$$h(\pi_1) \cdots h(\pi_{r_1}) < \frac{((r_1)!)^2}{2^{r_1 - 1} d_{\mathbb{K}}^{r_1}} h_{\mathbb{K}} R_{\mathbb{K}} \prod_{i=1}^{l} \log N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_i), \text{ (cf. Lemma 1)}$$

The element $\tau(x-\alpha)^{h_{\mathbb{K}}}$ can be written as

$$\tau(x-\alpha)^{h_{\mathbb{K}}} = \rho_0^{q_0} \cdot \pi_1^{q_1} \cdot \ldots \cdot \pi_{r_1}^{q_{r_1}},$$

where ρ_0 is a fixed generator of the group of roots of unity in $\mathbb{K}$ and $0 \leq q_0 \leq \omega_{\mathbb{K}} \leq 4n \log\log 6n$. Furthermore, using Lemma 4 we get

$$\log|x| \leq c_2 M^{3n} \log|b|, \quad (x \neq 0)$$

and by the second inequality of Lemma 1 we have

$$\begin{aligned}
\max_{1 \leq i \leq r_1} |q_i| &\leq \frac{((r_1)!)^3}{2^{r_1-1}} \left(\frac{6 d_{\mathbb{K}}^3}{\log d_{\mathbb{K}}} \right)^{r_1} (h(\tau) + h(x-\alpha)) h_{\mathbb{K}} R_{\mathbb{K}} \prod_{i=1}^{l} \log N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_i) \\
&\leq \frac{(n(s+1)-1)^{3(n(s+1)-1)}}{2} (6n^3)^{n(s+1)-1} M^{5n} \log|b| \prod_{i=1}^{l} \log N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_i) \\
&\leq \frac{(n(s+1)-1)^{3(n(s+1)-1)}}{2} (\log|b|)^{n(s+1)} M^{5n} \left(\frac{\sum_{i=1}^{l} \log N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_i)}{l} \right)^l \\
&\leq \frac{(n(s+1)-1)^{3(n(s+1)-1)}}{2} (\log|b|)^{n(s+1)} M^{5n} |b|^{\frac{n}{e}}.
\end{aligned}$$

Let $\beta \neq \alpha$ be a fixed zero of the minimal polynomial of α (over $\mathbb{Z}$) and σ be an automorphism of $\mathbb{C}$ with $\sigma(\alpha) = \beta$.

Set $t = r_1 + 1 \leq n(s+1)$,

$$\lambda = \frac{1}{(\beta-\alpha)\tau^{\frac{1}{h_{\mathbb{K}}}}}; \quad \mu = -\lambda$$

and write

$$\eta_0 = \rho,\ \eta_1 = \rho_0^{\frac{1}{h_{\mathbb{K}}}},\ \eta_2 = \pi_1^{\frac{1}{h_{\mathbb{K}}}}, \dots,\ \eta_{t-1} = \pi_{r_1}^{\frac{1}{h_{\mathbb{K}}}}$$

and

$$\psi_0 = \sigma(\rho),\ \psi_1 = (\sigma(\rho_0))^{\frac{1}{h_{\mathbb{K}}}},\ \psi_2 = (\sigma(\pi_1))^{\frac{1}{h_{\mathbb{K}}}}, \dots,\ \psi_{t-1} = (\sigma(\pi_{r_1}))^{\frac{1}{h_{\mathbb{K}}}},$$

where the $h_{\mathbb{K}}$th roots are fixed, ρ is a $h_{\mathbb{K}}$th primitive root of unity, furthermore, put

$$k_1 = q_0,\ k_1 = q_1, \dots,\ k_{t-1} = q_{r_1}.$$

Then the identity

$$\frac{x-\alpha}{\beta-\alpha} + \frac{x-\beta}{\alpha-\beta} = 1$$

implies

$$\lambda\eta_0^{k_0}\cdots\eta_{t-1}^{k_{t-1}} + \mu\psi_0^{k_0}\cdots\psi_{t-1}^{k_{t-1}} = 1 \tag{2}$$

with $k_0 \leq \omega_{\mathbb{K}} h_{\mathbb{K}}$.

Let $(x_1, z_1), \dots, (x_{t+2}, z_{t+2})$ be a subsequence of the solutions to (1) with $z_{i+1} - z_i \geq 6tn$ and $z_1 \geq 2tn + n^2$ and $k_j = (k_{0,j}, \dots, k_{t-1,j}) \in \mathbb{Z}^t$ the corresponding solution to (2), $j = 1, \dots, t+2$. It is easy to see that

$$K = \max_{\substack{0\leq i\leq t-1,\\ 1\leq j\leq t+1}} \{2, |k_{i,j+1} - k_{i,j}|\} \leq t^{3t}(\log b)^t M^{5n}|b|^{\frac{n}{e}}.$$

The first condition of Lemma 5 is trivial and since

$$\left|\frac{x_{j+1}-\alpha}{x_j-\alpha}\right| \geq \frac{1}{2}|b|^{\frac{z_{i+1}-z_i}{n}}$$

we have to prove that

$$|b|^{\frac{z_{i+1}-z_i}{n}} \geq |b|^{5t}M^{5n} \geq 18(t+1)^{\frac{t}{2}}t^{3t}(\log|b|)^t M^{5n} b^{\frac{n}{e}}$$

which is obvious by $|b| > c_4 M^{5n}$ and $t \le c(n) \log b$. Then Lemma 5 yields

$$|b|^{t+n} \le \frac{1}{2}|b|^{\frac{z_1}{n}} \le |x_1 - \alpha| \le \frac{1}{4}(t+1)^{\frac{t}{2}} K^t \le t^{4t} (\log b)^t M^{5n} |b|^{\frac{n}{e}},$$

which is a contradiction.

References

[BBH] A. Bérczes, B. Brindza and L. Hajdu, On power values of polynomials, *Publ. Math. Debrecen* (*to appear*).

[Be1] F. Beukers, On the generalized Ramanujan-Nagell equation I, *Acta Arith.* **38** (1981), 389–410.

[Be2] F. Beukers, On the generalized Ramanujan-Nagell equation II, *Acta Arith.* **39** (1981), 113–123.

[B&V] E. Bombieri and J. Vaaler, On Siegel's lemma, *Invent. Math.* **73** (1983), 11–32.

[B] B. Brindza, On S-integral solutions of the equation $y^m = f(x)$, *Acta Math. Hungar.* **44** (1984), 133–139.

[B1] B. Brindza, On the generators of S-unit groups in algebraic number fields, *Bull. Austral. Math. Soc.* **43** (1991), 325–329.

[BPPW] B. Brindza, Á. Pintér, A. van der Poorten and M. Waldschmidt, On the distribution of solutions of Thue's equations (*to appear*).

[B&Gy] B. Bugeaud and K. Győry, Bounds for the solutions of Thue-Mahler equations and norm form equations, *Acta Arith.* **74** (1996), 273–292.

[E] J. H. Evertse, Upper Bounds for the Numbers of Solutions of Diophantine Equations, Math. Centre Tract 168, Centre Math. Comp. Sci., *Amsterdam*, 1983.

[Gy] K. Győry, On the solutions of linear diophantine equations in algebraic integers in bounded norm, *Ann. Univ. Sci. Budapest, Eötvös Sect. Math.* **22/23** (1979-1980), 225–233.

[M] K. Mahler, An inequality for the discriminant of a polynomial, *Michigan Math. J.* **11** (1964), 257–262.

[ML1] L. Maohua, On the number of solutions of the diophantine equation $x^2 + D = p^n$, *C. R. Acad. Sci. Paris* **317** (1993), 135–138.

[ML2] L. Maohua, On the generalized Ramanujan-Nagell equation $x^2 - D = p^n$, *Acta Arith.* **58** (1991), 289–298.

[S] C. L. Siegel, Abschhätzung von Einheiten, *Nach. Akad. Wiss. Göttingen Math.-Phys.* **2** (1969), 71–86.

[Z] R. Zimmert, Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung, *Invent. Math.* **62** (1981), 367–380.

B. BRINDZA
INSTITUTE OF MATHEMATICS AND INFORMATICS
LAJOS KOSSUTH UNIVERSITY
H–4010 DEBRECEN P.O. BOX 12
HUNGARY

(Received September 23, 1997)