

The Catalan equation over finitely generated integral domains

By B. BRINDZA (Debrecen)

Dedicated to Professor Lajos Tamássy on his 70th birthday

Introduction

In 1976, TIJDEMAN [T] showed that the so-called Catalan equation

$$x^p - y^q = 1$$

has only finitely many rational integer solutions $x, y, p, q > 1$ and by using Baker's method an effectively computable upper bound for $\max\{x, y, p, q\}$ can be given. Later, VAN DER POORTEN [vdP] proved the p -adic analogue of the above result, and BRINDZA, GYÓRY and TIJDEMAN [BGy&T] extended Tijdeman's theorem to the case of algebraic number fields, that is, x and y are algebraic integers in an arbitrary but fixed algebraic number field. A further generalization when x and y are S -integers in an algebraic number field was proved by BRINDZA [B1] (see Lemma 2).

The purpose of this note is to give a further generalization of these results. After certain auxiliary steps the proof will be surprisingly simple.

Let G be a finitely generated extension of the rational number field $\mathbf{Q}$. Then G can be written as

$$G = \mathbf{Q}(z_1, \dots, z_r, u), \quad (r \geq 0)$$

where $\{z_1, \dots, z_r\}$ is a transcendence basis of G over $\mathbf{Q}$ and u is integral over the polynomial ring $\mathbf{Z}[z_1, \dots, z_r]$. Any element α of G has a unique representation (up to sign) in the form

$$(1) \quad \alpha = \frac{P_0 + P_1 u + \dots + P_{\delta-1} u^{\delta-1}}{P_{\delta}},$$

where δ is the degree of u over $\mathbf{Q}(z_1, \dots, z_r)$ and $P_0, \dots, P_\delta \in \mathbf{Z}[z_1, \dots, z_r]$ are relatively prime polynomials. Adopting the concepts and notation of GYÖRÝ [Gy2] we define the size of a non-zero polynomial $P \in \mathbf{Z}[z_1, \dots, z_r]$ as

$$s(P) = \max\{\log H(P), 1 + \max_{1 \leq i \leq r} \deg_{z_i} P\},$$

where $H(P)$ is the usual height of P , i.e. the maximum of the absolute values of its coefficients. The size of a non-zero $\alpha \in G$ written in the form (1) (with respect to the generating set $\{z_1, \dots, z_r, u\}$) is defined by

$$s(\alpha) = \max_{0 \leq i \leq \delta} \{s(P_i)\}.$$

It is clear that there are only finitely many elements in G with bounded size, and $s(\alpha)$ depends on the generating set. Let

$$R = \mathbf{Z}[\omega_1, \dots, \omega_t]$$

be a finitely generated subring of G . Then we have

Theorem. *All the solutions of the equation*

$$(2) \quad x^p - y^q = 1$$

in rational integers p, q and $x, y \in R$ with $p > 1$, $q > 1$, $pq > 4$ and x, y are not a root of unity, satisfy

$$\max\{p, q, s(x), s(y)\} < C,$$

where C is an effectively computable constant depending only on G and R .

It is easy to see that the conditions made on p, q, x and y are necessary.

Preliminaries

For fixed exponents p and q equation (2) can be considered as a special hyperelliptic equation. We may assume that G is a subfield of $\mathbf{C}$. Let $f(X) \in G[X]$ be a polynomial having zeros $\alpha_1, \dots, \alpha_k \in \mathbf{C}$ with multiplicities $r_1, \dots, r_k$, respectively. Moreover, let $m > 1$ be a rational integer and put

$$t_i = \frac{m}{(m, r_i)}, \quad i = 1, \dots, k.$$

Lemma 1. (BRINDZA [B2]) *Suppose that $\{t_1, \dots, t_k\}$ is not a permutation of the k -tuples*

$$\{t, 1, \dots, 1\}, \quad t \geq 1; \quad \{2, 2, 1, \dots, 1\}.$$

Then all the solutions of the equation

$$f(x) = y^m \quad \text{in } x, y \in R$$

satisfy

$$\max\{s(x), s(y)\} < C_1,$$

where C_1 is an effectively computable constant depending only on the generating set of G, R, f and m .

At this stage it may turn out to be useful to remark that R is not a Dedekind ring, generally, and hyperelliptic equations (over G) cannot be reduced to Thue-equations. The proof of Lemma 1 is based on Györy's specialization method. In [B2] it is assumed that f splits into linear factors over G , however, this technical assumption can be avoided; one can repeat the whole argument in the splitting field of f , which has the same transcendence degree, instead of G .

The following lemma corresponds to that special case of the Theorem, when $r = 0$, that is when G is an algebraic number field.

Let $\mathbf{K}$ be an algebraic number field, and S a finite set of (additive) valuations of $\mathbf{K}$. An element $\alpha \in \mathbf{K}$ is said to be S -integral if $v(\alpha) \geq 0$ for all valuations $v \notin S$. These elements of $\mathbf{K}$ form a ring which is denoted by $\mathcal{O}_{\mathbf{K},S}$. By the height $H(\alpha)$ of an algebraic number α we mean, as usual, the height of its minimal defining polynomial (over $\mathbf{Z}$).

Lemma 2. (BRINDZA [B1]) *All the solutions of equation (2) in rational integers p, q and $x, y \in \mathcal{O}_{\mathbf{K},S}$ with $p > 1, q > 1, pq > 4$ and x, y are not a root of unity, satisfy*

$$\max\{p, q, H(x), H(y)\} < C_2,$$

where C_2 is an effectively computable constant depending only on $\mathbf{K}$ and S .

Let k be an algebraically closed field of characteristic zero and $\mathbf{L}$ be a finite algebraic extension of the rational function field $k(t)$ with genus $g(\mathbf{L})$. For a non-zero element $\alpha \in \mathbf{L}$, the (additive) height $H_{\mathbf{L}/k}(\alpha)$ of α is defined by

$$H_{\mathbf{L}/k}(\alpha) = \sum_v \max\{0, v(\alpha)\}$$

where v runs through the (additive) valuations of $\mathbf{L}/k$ with value group $\mathbf{Z}$. It is easy to see that $H_{\mathbf{L}/k}(\alpha) \geq 0$ and $H_{\mathbf{L}/k}(\alpha) = 0$ if and only if $\alpha \in k$. Furthermore, we have

$$H_{\mathbf{L}/k}(\alpha^n) = |n|H_{\mathbf{L}/k}(\alpha), \quad n \in \mathbf{Z}.$$

Lemma 3. (MASON [M]) *Let $S = \{v_1, \dots, v_s\}$ be a finite set of valuations of $\mathbf{L}/k$ containing all the infinite valuations and let $\gamma_1, \gamma_2, \gamma_3$ be non-zero elements of $\mathbf{L}$ such that*

$$\gamma_1 + \gamma_2 + \gamma_3 = 0$$

and that $v(\gamma_1) = v(\gamma_2) = v(\gamma_3) = 0$ for all $v \notin S$. Then either $\gamma_1/\gamma_2 \in k$ or

$$H_{\mathbf{L}/k}(\gamma_1/\gamma_2) \leq s + 2g(\mathbf{L}) - 2.$$

We remark that a similar inequality had been proved by GYÖRY [Gy1] with larger constants.

Proof of the Theorem

Let x, y, p, q be an arbitrary solution to equation (2). We may assume that $r > 0$, for otherwise Lemma 2 implies the Theorem. Put

$$T_i = \{z_1, \dots, z_r\} \setminus \{z_i\} \quad \text{and} \quad k_i = \mathbf{Q}(T_i), \quad i = 1, \dots, r.$$

For a field k let $\bar{k}$ denote its algebraic closure and write

$$M_i = \bar{k}_i(z_i)(u^{(1)}, \dots, u^{(\delta)}), \quad i = 1, \dots, r,$$

where $u^{(1)}, \dots, u^{(\delta)}$ are the conjugates of u over $\mathbf{Q}(z_1, \dots, z_r)$. We show that

$$(3) \quad \bigcap_{i=1}^r \bar{k}_i = \overline{\mathbf{Q}}.$$

To do so we need the following simple observation. If $F_1 \subset F_2$ are fields and $\mu, \nu \in F_2$ algebraically independent over F_1 , then

$$\overline{F_1(\mu)} \cap \overline{F_1(\nu)} = \overline{F_1}$$

Indeed, let τ be an element of $\overline{F_1(\mu)} \cap \overline{F_1(\nu)}$ and suppose that $\tau \notin \overline{F_1}$. Then τ satisfies a polynomial relation

$$f_s \tau^s + \dots + f_1 \tau + f_0 = 0$$

with $f_i \in F_1[\mu]$, $i = 0, \dots, s$ and at least one f_i , $i \geq 0$, is not a constant in μ . Hence μ satisfies a similar non-trivial relation with coefficients from $F_1[\tau]$, that is $\mu \in \overline{F_1(\tau)}$ and the same argument gives $\nu \in \overline{F_1(\tau)}$ which is a contradiction, since μ and ν are algebraically independent over F_1 . After this we have

$$\bigcap_{i=1}^r \bar{k}_i = \bigcap_{i=2}^r (\bar{k}_i \cap \bar{k}_1) = \bigcap_{i=2}^r \overline{\mathbf{Q}(T_i \setminus \{z_1\})}$$

and one can obtain relation (3) by induction on the transcendence degree. We may assume that there exist an $i \in \{1, \dots, r\}$ such that $x \notin \bar{k}_i$, for otherwise $x \in \bar{k}_i$ and $y \in \bar{k}_i$, $i = 1, \dots, r$; hence x, y belong to the algebraic number field $\overline{\mathbf{Q}} \cap G$ and by applying Lemma 2 we have the Theorem.

If $x \notin \overline{k_i}$ for some i , then $y \notin \overline{k_i}$ and

$$\min\{H_{M_i/\overline{k_i}}(x), H_{M_i/\overline{k_i}}(y)\} \geq 1.$$

Let S denote the subset of valuations v of $M_i/\overline{k_i}$ containing all the infinite valuations, for which either $v(\omega_j) < 0$ holds for at least one $j \in \{1, \dots, t\}$, or $\max\{v(x), v(y)\} > 0$. Then we get $v(x) = v(y) = 0$ for all $v \notin S$ and

$$\begin{aligned} |S| &\leq \sum_{j=1}^t \sum_{v(\omega_j) < 0} 1 + \sum_{v(x) > 0} 1 + \sum_{v(y) > 0} 1 \leq \\ &\leq \sum_{j=1}^t H_{M_i/\overline{k_i}}(\omega_j) + H_{M_i/\overline{k_i}}(x) + H_{M_i/\overline{k_i}}(y). \end{aligned}$$

Now, we can consider equation (2) as an S -unit equation. Since $x^p \notin \overline{k_i}$ and $y^q \notin \overline{k_i}$, Lemma 3 yields

$$\begin{aligned} p - 2 + q - 2 &\leq (p - 2)H_{M_i/\overline{k_i}}(x) + (q - 2)H_{M_i/\overline{k_i}}(y) \leq \\ &\leq 2 \sum_{j=1}^t H_{M_i/\overline{k_i}}(\omega_j) + 4g(M_i/\overline{k_i}) - 4 \end{aligned}$$

and the genus of $M_i/\overline{k_i}$ can be estimated by the defining polynomial of u (cf. [Sch]).

Therefore, p and q are bounded and Lemma 1 completes the proof.

□

Acknowledgements. The author is grateful to Professor GYÖRY for his valuable remarks.

References

- [B1] B. BRINDZA, On S -integral solutions of the Catalan equation, *Acta Arith.* **48** (1987), 397–412.
- [B2] B. BRINDZA, On the equation $f(x) = y^m$ over finitely generated domains, *Acta Math. Hungar.* **53** (1989), 377–383.
- [BGy&T] B. BRINDZA, K. GYÖRY and R. TIJDEMAN, The Catalan equation over algebraic number fields, *J. reine angew. Math.* **367** (1986), 90–102.
- [Gy1] K. GYÖRY, Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains, *Acta Math. Hungar.* **42** (1983), 45–80.
- [Gy2] K. GYÖRY, Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains, *J. reine angew. Math.* **346** (1984), 54–100.
- [M] R.C. MASON, Diophantine Equations over Function Fields, LMS Lecture Notes, *Cambridge University Press* **96** (1984).
- [Sch] W.M. SCHMIDT, Thue's equation over function fields, *J. Austral Math. Soc (Series A)* **25** (1978), 385–422.

- [vdP] A.J. VAN DER POORTEN, Effectively computable bounds for the solutions of certain diophantine equations, *Acta Arith.* **33** (1977), 195–207.
[T] R. TIJDEMAN, On the equation of Catalan, *Acta Arith.* **29** (1976), 197–209.

B. BRINDZA
MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
DEBRECEN P.O. BOX 12
H-4010
HUNGARY

(Received Oktober 28, 1991)