Publ. Math. Debrecen
44 / 1–2 (1994), 183–187

On superelliptic equations

By J. VÉGSŐ (Debrecen)

To the memory of Professor András Rapcsák

Many numbertheoretical problems lead to superelliptic equations, i.e. equations of the type

$$f(x) = y^m. \tag{1}$$

SIEGEL [16], [17] and LE VEQUE [11] obtained general ineffective finiteness theorems for the integer solutions of (1) over algebraic number fields. For an ineffective extension to the case when the ground ring is an arbitrary integral domain of finite type over $\mathbb{Z}$ we refer to [10]. In the number field case BAKER [1] proved the first general effective result for superelliptic equations. Baker's theorem was improved and generalized by SPRINDZUK [18], TRELINA [19] and BRINDZA [2]. In the function field case effective bounds for the heights of the so-called S-integral solutions of (1) were given by SCHMIDT [14], MASON [12] and MASON and BRINDZA [13]. Using GYŐRY's specialization method (see [7], [8], [9]) Brindza extended his result to the case when the ground ring is a finitely generated domain (see Lemma 1). BRINDZA's bound depends on the parameters of the ground ring, the polynomial $f(X)$ and m. The purpose of this paper is to prove that the bound is independent of m.

We introduce some concepts and notation. Let G be a finitely generated extension field of the rational number field $\mathbb{Q}$. Then G can be written in the form

$$G = \mathbb{Q}(z_1, \dots, z_q, u),$$

where $\{z_1, \dots, z_q\}$ is a transcendence basis of G over $\mathbb{Q}$ and u is integral over the polynomial ring $\mathbb{Z}[z_1, \dots, z_q]$.

Let

$$F(X) = X^\delta + F_1 X^{\delta-1} + \ldots + F_\delta$$

be the minimal polynomial of u over $\mathbb{Q}(z_1, \dots z_q)$. For brevity let us write

$$D = \max_i \deg F_i, L = \max_i L(F_i),$$

where $L(P)$ denotes the lenght of the polynomial $P \in \mathbb{Z}[z_1, \ldots, z_q]$ (i.e. the sum of the absolute values of the coefficients of P). Since $\mathbb{Z}[z_1, \ldots, z_q]$ is integrally closed, all F_i lie in $\mathbb{Z}[z_1, \ldots, z_q]$.

Any element α of G can be written in the form

$$\alpha = \frac{P_0 + P_1 u + \ldots + P_{\delta-1} u^{\delta-1}}{Q}$$

where $P_0, \ldots, P_{\delta-1}$ and Q are (up to the factors ± 1) uniquely determined relatively prime polynomials from $\mathbb{Z}[z_1, \ldots, z_q]$. Let Deg P denote the total degree in $z_1, \ldots, z_q$ of an element P of $\mathbb{Z}[z_1, \ldots, z_q]$ and define the *degree* of α as

$$\operatorname{Deg} \alpha = \max\{\operatorname{Deg} P_0, \ldots, \operatorname{Deg} P_{\delta-1}, \operatorname{Deg} Q\}.$$

The *size* of $\alpha \neq 0$ (with respect to the generating set $\{z_1, \ldots, z_q, u\}$ of G) will be defined as

$$s(\alpha) = \max\{s(P_0), \ldots, s(P_{\delta-1}), s(Q)\}$$

where

$$s(P) = \max\{\log H(P), 1 + \max_i \deg_{z_i} P\}$$

and $H(P)$ denotes the height of $P \in \mathbb{Z}[z_1, \ldots, z_q]$ (i.e. the maximum of the absolute values of the coefficients of P). It is clear that there are only finitely many elements in G with bounded size. Let $R = \mathbb{Z}[u_1, \ldots, u_t]$ be a finitely generated subring of G. Further, let $f \in G[X]$ be a polynomial having all its roots in G. We assume throughout that

$$f(X) = a \prod_{i=1}^{n} (X - \alpha_i)^{r_i}$$

with $a \neq 0, n > 0$ and $\alpha_i \neq \alpha_j$ for $i \neq j$. Let $m > 1$ be an integer and consider the equation

$$f(x) = y^m \quad \text{in} \quad x, y \in R. \tag{2}$$

To avoid some technical difficulties, we shall consider the solutions of (2) in the larger subring

$$R_1 = \mathbb{Z}\left[z_1, \ldots, z_q, \frac{1}{b}, u\right]$$

of G where b denotes the product of the denominators of $a, \alpha_1, \ldots, \alpha_n, u_1, \ldots, u_t$. It is easy to see that $b \in \mathbb{Z}[z_1, \ldots, z_q]$ and $R \subseteq R_1$. In the special case when $q = 0$ and $\{u_1, \ldots, u_t\}$ is an integral basis of G then R is just the ring of integers of G.

We shall give an effectively computable bound for the size of the solutions x, y in R_1, which depends only on G, R_1 and f.

Theorem. *Put* $t_i = m/(m, r_i)$ *for* $i = 1, \dots, n$ *and suppose that* $\{t_1, \dots, t_n\}$ *is not a permutation of the* n*-tuplets*

$$(a) \quad \{t, 1, \dots, 1\} \qquad \text{and} \qquad (b) \quad \{2, 2, 1, \dots, 1\}.$$

Then all the solutions $x, y \in R_1$ *of the equation* (2) *satisfy*

$$\max\{s(x), s(y)\} < c_1$$

where c_1 *is an effectively computable constant depending only on* G, R_1, $f(X)$.

Auxiliary results

To prove our Theorem we need some lemmas.

Lemma 1. *Under the assumptions of the Theorem all the solutions* $x, y \in R_1$ *of* (2) *satisfy*

$$\max\{s(x), s(y)\} < c_2$$

where c_2 *is an effectively computable constant depending only on* G, R_1, $f(X)$ *and* m.

Proof. This is the Theorem in [3].

Let L be an algebraic number field and let

$$g_0 \prod_{i=1}^{r} (X - \gamma_i)^{r_i} = g(X) \in L[X]$$

be a given polynomial where $r \geq 1, g_0 \neq 0$ and the γ_i'-s are distinct elements of the splitting field of g. Further, let $\mathfrak{p}_1, \dots, \mathfrak{p}_s (s \geq 0)$ be distinct prime ideals in L and denote by S the set of all the infinite valuations and all the (additive) valuations of L corresponding to $\mathfrak{p}_1, \dots, \mathfrak{p}_s$. We recall that an element α of L is said to be an S-integer if $v(\alpha) \geq 0$ for every valuation $v \notin S$. The set of S-integers is denoted by O_S.

Lemma 2. *Suppose that* $g(X)$ *has at least two distinct zeros and* $y \neq 0$ *is not a root of unity. Then the equation*

$$f(x) = y^m \quad \text{in} \quad x, y \in O_S, m \in \mathbb{Z}, \quad \text{with} \quad m \geq 2$$

implies that $m < c_3$, *where* c_3 *is an effectively computable constant depending only on* S, g *and* L.

Proof. See [5] Theorem 4 and [15] Theorem 10.3.

Now let k be an algebraically closed field of characteristic 0, and let K be a finite algebraic extension of the rational function field $k(t)$ with

genus $g(K)$ and let $P(X) \in K[X]$. For $x \neq 0$ in K, the height $H_K(x)$ of x is defined by

$$H_K(x) = -\sum_v \min\{0, v(x)\}$$

where v runs through the valuations of K/k with value group $\mathbb{Z}$.

Lemma 3. *If $P(X)$ has at least two distinct zeros (in the splitting field of P) then all the solutions of the equation*

$$P(x) = y^m \quad \text{in} \quad x, y \in K \quad \text{with} \quad y \notin k$$

satisfy $m < c_4$, where c_4 is an effectively computable constant depending only on $g(K)$ and the polynomial $P(X)$.

Proof. This is the main result in [6].

Lemma 4. *Let $f(X) \in G[X]$ be a polynomial with at least two distinct zeros. Suppose $m \geq 0, x, y \in R_1$ and y is not a root of unity. Then the equation*

$$f(x) = y^m$$

implies that m is bounded by an effectively computable constant depending only on f, R_1 and G.

Proof. Let $x, y \in R_1$, and $m \in \mathbb{Z}$ with $m \geq 2$ an arbitrary but fixed solution of (2). We have two cases to distinguish. In the case $q = 0$ Lemma 4 is a simple consequence of Lemma 2. In the sequel, we assume that $q > 0$. Set $T_i = \{z_1, \ldots, z_q\} \setminus \{z_i\}$ and $k_i = \mathbb{Q}(T_i)$, further denote by $\overline{k_i}$ the algebraic closure of the field k_i in a fixed algebraic closure of G. Then we obtain

$$\bigcap_{i=1}^{q} \overline{k_i} = \overline{\mathbb{Q}} \qquad \text{(cf. Brindza [4])}.$$

If $y \in \bigcap_{i=1}^q \overline{k_i}$ then one can see that x and y are S-integers in a fixed and determinable algebraic number field and we can apply Lemma 2. If $y \notin \bigcap_{i=1}^q \overline{k_i}$ then there exists an index $j\,(1 \leq j \leq q)$ for which $y \notin \overline{k_j}$, however $y \in \overline{k_j}(z_j)$. Let K be the splitting field of the polynomial f over the field $\overline{k_i}(z_i)$. K is an algebraic function field over $\overline{k_i}$ and Lemma 3 completes the proof of Lemma 4.

Proof of the Theorem. Adopting the above notation, if y is a root of unity then the size of y is bounded and y^m is an element of a cyclic group with a finite and determinable order. The solution x is a zero of the polynomial $f(X) - y^m$ thus its size is bounded (for the known properties of the size we refer to [8]). Finally, if y is not a root of unity, our Theorem is a consequence of Lemmas 1 and 4.

References

[1] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* **65** (1969), 439–444.

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

[3] B. Brindza, On the equation $f(x) = y^m$ over finitely generated domains, *Acta Math. Hungar.* **53** (1989), 377–383.

[4] B. Brindza, The Catalan equation over finitely generated integral domains, *Publ. Math. Debrecen* **42** (1993), 193–198.

[5] B. Brindza, Zeros of polynomials and exponential diophantine equations, *Compos. Math.* **61** (1987), 137–157.

[6] B. Brindza, Á. Pintér and J. Végső, The Schinzel-Tijdeman theorem over function fields, (*in preparation*).

[7] K. Győry, Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated domains, *Acta Math. Hungar.* **42** (1983), 45–80.

[8] K. Győry, 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.

[9] K. Győry, Effective finiteness theorems for diophantine problems and their applications, Academic doctoral dissertation, 1983. (in Hungarian)

[10] S. Lang, Diophantine geometry, Interscience Tracts in Pure and Applied Mathematics, No. 11, *New York—London*, 1962.

[11] W. J. LeVeque, On the equation $y^m = f(x)$, *Acta Arith.* **9** (1964), 209–219.

[12] R. C. Mason, The hyperelliptic equation over function fields, *Math. Proc. Camb. Philos. Soc.* **93** (1983), 219–230.

[13] R. C. Mason and B. Brindza, LeVeque's superelliptic equation over function fields, *Acta Arith.* **47** (1986), 167–173.

[14] W. M. Schmidt, Thue's equation over function fields, *J.Austral Math. Soc.* **A 25** (1978), 385–422.

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

[16] C. L. Siegel, The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$, *J. London Math. Soc.* **1** (1926), 66–68.

[17] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss.*, 1929, pp. 1–41.

[18] V. G. Sprindzuk, A hyperelliptic diophantine equation and class numbers, *Acta Arith.* **30** (1976), 95–108. (in Russian)

[19] L. A. Trelina, On S-integral solutions of the hyperelliptic equation, *Dokl. Akad. Nauk. BSSR* **22** (1978), 881–884. (in Russian)

J. VÉGSŐ
KOSSUTH LAJOS UNIVERSITY,
DEBRECEN, P.O. BOX 12.,
4010–HUNGARY

(Received November 25, 1992)