УДК 511.42 DOI 10.22405/2226-8383-2016-17-4-180-184

PROBLEM OF NESTERENKO AND METHOD OF BERNIK

N. V. Budarina (Khabarovsk), H. O'Donnell (Dublin)

Dedicated to Yuri Valentinovich Nesterenko and Vasilii Ivanovich Bernik on their 70th birthdays

Abstract

In this article we prove that, if integer polynomial P satisfies $|P(\omega)|_p < H^{-w}$, then for $w > 2n-2$ and sufficiently large H the root γ belongs to the field of p-adic numbers.

Keywords: integer polynomials, discriminants of polynomials.

Bibliography: 16 titles.

1. Introduction

Throughout this paper, p is a prime number, $\mathbb{Q}_p$ is the field of p-adic numbers,

$$P(x) = a_n x^n + \ldots + a_1 x + a_0$$

is an integer polynomial with degree $\deg P(x) = n$ and height $H(P) = \max_{0 \leqslant j \leqslant n} |a_j|$. We denote by $\mathcal{P}_n$ the set of integer polynomials of degree n. Let $\mathcal{P}_n(H) = \{P \in \mathcal{P}_n : H(P) = H\}$.

In this paper, a result originally considered by Y. V. Nesterenko is examined. In [1] Y.V. Nesterenko discussed the solvability of the equation $P(x) = 0$ in the ring of p-adic integers $\mathbb{Z}_p$ and proved the following result.

Theorem 1. *Let x be an integer and $P \in \mathcal{P}_n(H)$. If*

$$|P(x)|_p \leqslant e^{-8n^2} H^{-4n},$$

then there exists a p-adic number γ such that

$$P(\gamma) = 0, \quad |x - \gamma|_p < 1.$$

Note that a similar problem was considered in [2] and there was given a criteria for when the closest root of a polynomial to a real point belongs to the field of real numbers. Knowledge of the nature of the roots is very important in the problems of Diophantine approximations for construction of regular systems [3, 4]. Numerous applications of this concept arose when obtaining estimates for the Hausdorff measure and Hausdorff dimension of Diophantine sets [5] and proving analogues of the Khintchine theorem [6, 7]. Using the regular systems, the exact theorems on approximation of real numbers by real algebraic [6], by algebraic integers [8], of complex numbers by complex algebraic [9] were obtained, and similar problems in the field of p-adic numbers [10] and in $\mathbb{R} \times \mathbb{C} \times \mathbb{Q}_p$ [7] were investigated.

The Theorem 1 can be improved for p-adic leading polynomials. Such a polynomial $P \in \mathcal{P}_n$ satisfies

$$|a_n|_p \gg 1. \tag{1}$$

Theorem 2. *Let $\omega \in \mathbb{Z}_p$ and $P \in \mathcal{P}_n(H)$ be a p-adic leading polynomial. Then if*

$$|P(\omega)|_p < H^{-w} \tag{2}$$

for $w > 2n-2$, and for sufficiently large $H > H_0(n)$, it follows that the root γ_1 of P belongs to $\mathbb{Q}_p$ and

$$|\omega - \gamma_1|_p < 1. \tag{3}$$

Remark 1. *If $D(P) \neq 0$ then we have that the root γ_1 of P is closest to $\omega \in \mathbb{Z}_p$.* The above theorem will be proved using a general method of V.I. Bernik which was developed in [11, 12].

2. Preliminary setup and auxilliary Lemmas

Let $P \in \mathcal{P}_n$ have roots $\gamma_1, \gamma_2, \ldots, \gamma_n$ in $\mathbb{Q}_p^*$, where $\mathbb{Q}_p^*$ is the smallest field containing $\mathbb{Q}_p$ and all algebraic numbers. Then, from (1) it follows that

$$|\gamma_i|_p \ll 1, \quad i = 1, \ldots, n; \tag{4}$$

i.e. the roots are bounded. This follows from Lemma 4 in ([13], p.85).

Define the sets

$$T_p(\gamma_k) \;\; = \;\; \{\omega \in \mathbb{Z}_p : |\omega - \gamma_k|_p = \min_{1 \leqslant i \leqslant n} |\omega - \gamma_i|_p\}, \;\; 1 \leqslant k \leqslant n.$$

Consider the set $T_p(\gamma_k)$ for a fixed k and for ease of notation assume that $k = 1$. Next, reorder the other roots so that

$$|\gamma_1 - \gamma_2|_p \;\; \leqslant \;\; |\gamma_1 - \gamma_3|_p \;\; \leqslant \ldots \leqslant \;\; |\gamma_1 - \gamma_n|_p.$$

Fix $\epsilon > 0$ where ϵ is sufficiently small and suppose that $\epsilon_1 = \epsilon N^{-1}$ where $N = N(n) > 0$ is sufficiently large. Let $T = [\epsilon_1^{-1}]$.

For a polynomial $P \in \mathcal{P}_n(H)$ define the real numbers ρ_j by

$$|\gamma_1 - \gamma_j|_p \;\; = \;\; H^{-\rho_j}, \;\; 2 \leqslant j \leqslant n, \quad \rho_2 \geqslant \rho_3 ... \geqslant \rho_n.$$

Define the integers m_j, $2 \leqslant j \leqslant n$, such that

$$\frac{m_j - 1}{T} \leqslant \rho_j < \frac{m_j}{T}, m_2 \geqslant m_3 \geqslant ... \geqslant m_n \geqslant 0.$$

Further define numbers s_i such that

$$s_i \;\; = \;\; \frac{m_{i+1} + \ldots + m_n}{T}, \quad (1 \leqslant i \leqslant n-1), \;\; s_n = 0.$$

The first Lemma is a p-adic analogue of the Lemma, which was proved by Bernik in [14] and is a generalisation of Sprindžuk's Lemma ([13], p.77).

Lemma 1. *[15] Let $\omega \in T_P(\gamma_1)$. Then*

$$|\omega - \gamma_1|_p \leqslant \min_{1 \leqslant j \leqslant n} (|P(\omega)|_p |P'(\gamma_1)|_p^{-1} \prod_{k=2}^{j} |\gamma_1 - \gamma_k|_p)^{1/j}.$$

The following Lemma is often referred to as Gelfond's Lemma.

Lemma 2 ([16], Lemma A.3). *Let $P_1, P_2, \ldots, P_k$ be polynomials of degree $n_1, \ldots, n_k$ respectively, and let $P = P_1 P_2 \ldots P_k$. Let $n = n_1 + n_2 + \ldots + n_k$. Then*

$$2^{-n} H(P_1) H(P_2) \ldots H(P_k) \leqslant H(P) \leqslant 2^n H(P_1) H(P_2) \ldots H(P_k).$$

In the proof of theorem we will refer to the following statement known as Hensel's Lemma.

Lemma 3 ([4], p. 134). *Let P be a polynomial with coefficients in $\mathbb{Z}_p$, let $\xi = \xi_0 \in \mathbb{Z}_p$ and $|P(\xi)|_p < |P'(\xi)|_p^2$. Then as $n \to \infty$ the sequence*

$$\xi_{n+1} = \xi_n - \frac{P(\xi_n)}{P'(\xi_n)}$$

tends to some root $\beta \in \mathbb{Q}_p$ of the polynomial P and

$$|\beta - \xi|_p \leqslant |P(\xi)|_p / |P'(\xi)|_p^2 < 1.$$

3. Proof of Theorem 2

Two cases must be dealt with separately: $D(P) \neq 0$ and $D(P) = 0$.

3.1. Case I: $D(P) \neq 0$

First consider a polynomial $P \in \mathcal{P}_n(H)$ satisfying $D(P) \neq 0$ and (2), and assume that $|P'(\omega)|_p^2 \leqslant |P(\omega)|_p$. We will obtain a contradiction. Using (4), we get $|P'(\omega)|_p < H^{-w/2}$.

It is well known that $|D(P)| = \frac{|\Delta|}{|a_n|}$, where

$$\Delta = \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \\ na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \dots & a_1 & \dots & 0 & \dots & 0 \\ 0 & na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \dots & a_1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \dots & a_1 \end{pmatrix}.$$

Hence the determinant,

$$\begin{aligned} |\Delta| &\leqslant |a_n|((2n-2)!(nH)^{2n-2} + n(2n-2)!(nH)^{2n-2}) \\ &= |a_n|(2n-2)!(n+1)(nH)^{2n-2} \leqslant 2n^{2n-1}(2n-2)!H^{2n-2}|a_n|, \end{aligned}$$

using the fact that $|a_i| \leqslant H$, $i = 0, 1, \dots, n$. Thus, $|D(P)| \leqslant 2n^{2n-1}(2n-2)!H^{2n-2}$. This implies that

$$|D(P)|_p \geqslant 2^{-1}n^{1-2n}((2n-2)!)^{-1}H^{-2n+2}. \tag{5}$$

Using Lemma 1, $|a_n|_p \gg 1$ and (2),

$$\begin{aligned} |\omega - \gamma_1|_p &\leqslant \min_{1 \leqslant j \leqslant n}(|P(\omega)|_p|P'(\gamma_1)|_p^{-1}\textstyle\prod_{k=2}^{j}|\gamma_1 - \gamma_k|_p)^{1/j} \\ &< \min_{1 \leqslant j \leqslant n}(H^{-w}|a_n|_p^{-1}\textstyle\prod_{k=j+1}^{n}|\gamma_1 - \gamma_k|_p^{-1})^{1/j} \\ &\leqslant \min_{1 \leqslant j \leqslant n}(H^{-w}|a_n|_p^{-1}H^{s_j})^{1/j} \\ &\ll \min_{1 \leqslant j \leqslant n} H^{\frac{-w+s_j}{j}}. \end{aligned}$$

Define $\sigma(P)$ as the cylinder of points w satisfying

$$|\omega - \gamma_1|_p \ll \min_{1 \leqslant j \leqslant n} H^{\frac{-w+s_j}{j}}.$$

Let $\theta_j = \frac{w-s_j}{j}$ and denote by θ_0 the maximum value of θ_j, $j = 1, \dots, n$.

Now the polynomial P' is expanded as a Taylor series and each term is estimated on $\sigma(P)$. Thus

$$\begin{aligned} P'(\omega) &= P'(\gamma_1) + \sum_{j=2}^{n}((j-1)!)^{-1}P^{(j)}(\gamma_1)(\omega-\gamma_1)^{j-1}, \\ |P^{(j)}(\gamma_1)(\omega-\gamma_1)^{j-1}|_p &\ll H^{-s_j+(n-j)\epsilon_1}H^{-\theta_0(j-1)}. \end{aligned}$$

As $\theta_0 \geqslant \theta_j$, this implies that

$$|P^{(j)}(\gamma_1)(\omega-\gamma_1)^{j-1}|_p \ll H^{-s_j+(n-j)\epsilon_1+\frac{j-1}{j}(-w+s_j)} \leqslant H^{-w/2+(n-2)\epsilon_1} \quad \text{for } 2 \leqslant j \leqslant n.$$

Thus,

$$|P'(\gamma_1)|_p \leqslant \max_{1 \leqslant j \leqslant n}\{|P^{(j)}(\gamma_1)(\omega-\gamma_1)^{j-1}|_p\} \ll H^{-w/2+(n-2)\epsilon_1}$$

for $H > H_0(n)$.

Expressing the discriminant $D(P)$ in the form

$$|D(P)|_p = |a_n|_p^{2n-2} \prod_{1\leqslant i<j\leqslant n} |\gamma_i - \gamma_j|_p^2 = |a_n|_p^{2n-4} |P'(\gamma_1)|_p^2 \prod_{2\leqslant i<j\leqslant n} |\gamma_i - \gamma_j|_p^2$$

and using the facts that $|\gamma_i|_p \ll 1$ and $|a_n|_p \leqslant 1$, we obtain

$$|D(P)|_p \ll |P'(\gamma_1)|_p^2.$$

This contradicts (5) for $w > 2n-2+2(n-2)\epsilon_1$ and sufficiently large H. Therefore, $|P'(\omega)|_p^2 > |P(\omega)|_p$ holds for $w > 2n-2+2(n-2)\epsilon_1$, and case I follows immediately from Lemma 3. Hence, there exists a root $\gamma_1 \in \mathbb{Q}_p$ of P such that $|\omega - \gamma_1|_p \leqslant |P(\omega)|_p / |P'(\omega)|_p^2 < 1$.

3.2. Case II: $D(P) = 0$

Consider the polynomial $P \in \mathcal{P}_n$ satisfying $D(P) = 0$. First, P is decomposed into irreducible polynomials $T_i(\omega) \in \mathbb{Z}[\omega]$, i.e.

$$P(\omega) = \prod_{i=1}^{k} T_i^{s_i}(\omega).$$

It will be shown that for some index j, $1 \leqslant j \leqslant k$,

$$|T_j(\omega)|_p < 2^{nw/2} H^{-w}(T_j). \tag{6}$$

Assume the opposite, so that

$$|T_j(\omega)|_p \geqslant 2^{nw/2} H^{-w}(T_j) \text{ for all } j,\ 1 \leqslant j \leqslant k.$$

Then, by Lemma 2,

$$|P(\omega)|_p \geqslant \prod_{j=1}^{k} (2^{nw/2} H^{-w}(T_j))^{s_j} \geqslant 2^{nw(\sum_{j=1}^{k} s_j/2-1)} H(P)^{-w} \geqslant H(P)^{-w}$$

which contradicts (2). Thus (6) holds.

Hence, applying the same method as in Case I for T_j, $D(T_j) \neq 0$, which satisfies (6), it follows that there exists a p-adic number γ_1 such that $|\omega - \gamma_1|_p < 1$ and $T_j(\gamma_1) = 0$. This implies $P(\gamma_1) = 0$. □

REFERENCES

1. Y. V. Nesterenko, *Roots of polynomials in p-adic fields.* Preprint.

2. N. Budarina, H. O'Donnell, *On a problem of Nesterenko: when is the closest root of a polynomial a real number?* International Journal of Number Theory, 8 (2012), no. 3, 801–811.

3. A. Baker and W.M. Schmidt, *Diophantine approximation and Hausdorff dimension*, Proc. Lond. Math. Soc. 21 (1970), 1–11.

4. V. I. Bernik, M. M. Dodson, *Metric Diophantine approximation on manifolds*, Cambridge Tracts in Math., vol. 137, Cambridge Univ. Press, 1999.

5. H. Dickinson and S. Velani, *Hausdorff measure and linear forms*, J. reine angew. Math., 490 (1997), 1–36.

6. V. Beresnevich, *On approximation of real numbers by real algebraic numbers*, Acta Arith. 90 (1999), 97–112.

7. V. Bernik, N. Budarina and D. Dickinson, *A divergent Khintchine theorem in the real, complex, and p-adic fields*, Lith. Math. J. 48 (2008), no. 2, 158–173.

8. Y. Bugeaud, *Approximation by algebraic integers and Hausdorff dimension*, J. Lond. Math. Soc., 65 (2002), pp. 547–559.

9. V. I. Bernik and D. Vasiliev, *Khintchine theorem for the integer polynomials of complex variable*, Tr. Inst. Mat. Nats. Akad. Navuk Belarusi, 3 (1999), 10–20.

10. V. V. Beresnevich, V. I. Bernik and E. I. Kovalevskaya, *On approximation of p-adic numbers by p-adic algebraic numbers*, J. Number Theory, 111 (2005), no. 1, 33–56.

11. V. Bernik, *An application of Hausdorff dimension in the theory of Diophantine approximation*, Acta Arith. 42 (1983), 219–253.

12. V. Bernik, *On the exact order of approximation of zero by values of integral polynomials*, Acta Arith. 53 (1989), 17–28.

13. V. Sprindžuk, *Mahler's problem in the metric theory of numbers*, vol. 25, Amer. Math. Soc., Providence, RI, 1969.

14. V. I. Bernik, *The metric theorem on the simultaneous approximation of zero by values of integer polynomials*, Izv. Akad. Nauk SSSR, Ser. Mat. 44 (1980), 24–45.

15. V. Bernik, D. Dickinson and J. Yuan, *Inhomogeneous diophantine approximation on polynomials in* $\mathbb{Q}_p$, Acta Arith., 90 (1999), no. 1, 37–48.

16. Y. Bugeaud, *Approximation by algebraic numbers*, Cambridge Tracts in Mathematics, Cambridge, 2004.

Khabarovsk Division of Institute for Applied Mathematics
Dublin Institute of Technology

Получено 28.11.2016 г.
Принято в печать 12.12.2016 г.