On the divisibility of the discriminant of an integer polynomial by prime powers.

October 14, 2008

V. Bernik
Institute of Mathematics, Surganova str. 11, 220072, Minsk, Belarus
(e-mail: bernik@im.bas-net.by)
F. Götze
Universität Bielefeld, Fakultät für Mathematik, Postfach 10 01 31, 33501 Bielefeld, Germany
(e-mail: goetze@math.uni-bielefeld.de)
O. Kukso
Institute of Mathematics, Surganova str. 11, 220072, Minsk, Belarus
(e-mail: olga_kukso@tut.by)

Abstract

Let $P \in \mathbb{Z}[t]$ with $\deg P \leqslant n$ and height $H = H(P)$. Let $|w|_p$ be the p–adic valuation of $w \in \mathbb{Q}_p$. Also define K to be a cylinder in $\mathbb{Q}_p$ and a set $B \subset K$. The Haar measure of B is denoted by μB.

In this article we obtain a lower bound for the number of polynomials with fixed degree and height whose discriminants are multiples of large prime powers. The basic idea of the proof concerns the simultaneous metric theory of the size of integer polynomials and their derivatives. Namely, it is shown that for a given number c_0 and constants c_1, c_2 with $c_1c_2 < c_0$ the system of inequalities

$$\begin{cases} |P(w)|_p < c_1 Q^{-n-1+v}, \\ |P'(w)|_p < c_2 Q^{-v}, \\ H(P) \leqslant Q \end{cases}$$

has solutions $P \in \mathbb{Z}[t]$ only for a set $B = \{w\}$ with $\mu B \leqslant \frac{1}{2}\mu K$.

Keywords: Diophantine approximation, discriminant, p–adic valuation, Haar measure.

The basic characteristic of a real number is considered to be its value. For natural numbers q the same we could consider one of its basic characteristics to be its arithmetic structure. By this, we mean the canonical decomposition of q into its unique product of primes. It is well-known that the factorization of sufficiently large natural numbers demands a lot of computer time. The discriminant value may grow quickly with the growth of degree and height.

Let $P \in \mathbb{Z}[x]$ be of the form

$$P(x) = a_n x^n + \cdots + a_1 x + a_0, \quad H = H(P) = \max_{0 \leqslant j \leqslant n} |a_j|. \tag{1}$$

Here, H denotes the height of the polynomial P. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of P. Then the discriminant $D(P)$ of P is defined as

$$D(P) = a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2. \tag{2}$$

The discriminant of the polynomial is a symmetric function of its roots. As it concerns the product of the square of the distances between the roots multiplied by a_n^{2n-2} it is in fact a polynomial of the coefficients of P and is therefore an integer. The discriminant $D(P)$ can also be written as the determinant of a matrix of order $2n-1$ (for details see [12]). Therefore discriminant calculating for general polynomials with large n and H is hard to perform. Taking this into account and assuming that $D(P) \neq 0$ we obtain that there exists a constant $c(n)$ such that

$$1 \leqslant |D(P)| < c(n) H^{2n-2}. \tag{3}$$

Several papers, see [2 – 4], are devoted to the study of the set of possible values of the discriminants. In this article we ask: how often is $D(P)$ divisible by the power of a chosen prime p. The main method used is the metric theory of p–adic Diophantine approximation, the basis of which was developed by V.G. Sprindžuk in [4] when he considered Mahler's conjecture and its analogue in the field of p–adic numbers.

Throughout the paper we will need the following notation. Let $p \geqslant 2$ be a fixed prime number with $\mathbb{Q}_p$ the field of p–adic numbers and $|w|_p$ the p–adic valuation of $w \in \mathbb{Q}_p$. Let $\mathbb{A}_{p,n}$ be the set of algebraic numbers of degree n lying in $\mathbb{Q}_p$, $\mathbb{A}_p$ be the set of all algebraic numbers and finally, $\mathbb{Q}_p^*$ be the extension of $\mathbb{Q}_p$ containing $\mathbb{A}_p$. There is a natural extension of the p–adic valuation from $\mathbb{Q}_p$ to $\mathbb{Q}_p^*$, see [11, 6, 8]. This valuation will also be denoted by $|\cdot|_p$. The disc in $\mathbb{Q}_p$ of radius r centred at α is the set of solutions of the inequality $|x - \alpha|_p < r$. The Haar measure of a set $S \subset \mathbb{Q}_p$ will be denoted by $\mu(S)$. The notation $X \ll Y$ will mean $X = O(Y)$ and $X \asymp Y$ means $X \ll Y \ll X$.

In 1989 Bernik [3] proved A. Baker's conjecture by showing that for almost all $x \in \mathbb{R}$ the inequality $|P(x)| < H(P)^{-n+1} \Psi(H(P))$ has only finitely many solutions in $P \in \mathbb{Z}[x]$ with $\deg P \leqslant n$ whenever $\Psi : \mathbb{N} \to \mathbb{R}_+$ is monotonic and the sum

$$\sum_{h=1}^{\infty} \Psi(h) \tag{4}$$

converges. In 1999 Beresnevich [1] showed that if the sum in (4) diverges then the inequality has infinitely many solutions. These results of Bernik and Beresnevich have been generalised to the p–adic case, see [9, 2].

In this article we develop methods that were initially proposed in [11, 3, 1]. More precisely, for sufficiently large $Q \in \mathbb{R}$ we obtain a lower bound for the number of polynomials in the set

$$\mathcal{P}_n(Q) = \{P(x) \mid \deg P \leqslant n,\ H(P) \leqslant Q\}, \tag{5}$$

whose discriminants are divisible by large powers of a fixed prime number.

Theorem 1 *There are at least $c(n)Q^{n+1-2v}$ polynomials $P \in \mathcal{P}_n(Q)$ with discriminants $D(P)$ satisfying*

$$|D(P)|_p < Q^{-2v},$$

where $v \in [0, \frac{1}{2}]$.

Theorem 2 *Let Q denote a sufficiently large number and c_1 and c_2 denote constants depending only on n. Also, let K be a disc in $\mathbb{Q}_p$. Assume that $c_1c_2 < 2^{-n-9}p^{-6}$ and $v \in [0, \frac{1}{2}]$. If $M_{n,Q}(c_1, c_2)$ is the set of $w \in K \subset \mathbb{Q}_p$ such that the system of inequalities*

$$\begin{cases} |P(w)|_p < c_1Q^{-n-1+v}, \\ |P'(w)|_p < c_2Q^{-v} \end{cases}$$

has solutions in polynomials $P \in \mathcal{P}_n(Q)$, then

$$\mu(M_{n,Q}(c_1, c_2)) < \frac{\mu(K)}{2}.$$

Auxiliary statements. The following lemmas are necessary for the proof of the theorems. After stating them we will show how Theorem 1 can be obtained from Theorem 2.

Lemma 1 *Let α_1 be the nearest root of a polynomial P to $w \in \mathbb{Q}_p$. Then*

$$|w - \alpha_1|_p \leqslant |P(w)|_p|P'(w)|_p^{-1}, \tag{6}$$

and

$$|w - \alpha_1|_p \leqslant \min_{2\leqslant j\leqslant n} \left(|P(w)|_p|P'(w)|_p^{-1} \prod_{k=2}^{j} |\alpha_1 - \alpha_j|_p \right)^{\frac{1}{j}}, \tag{7}$$

where $|\alpha_1 - \alpha_2|_p \leqslant |\alpha_1 - \alpha_j|_p$ for $2 \leqslant j \leqslant n$.

For the proof see [11, 3, 5].

Lemma 2 *Let $\delta > 0$ and $E(\delta)$ be the set of $w \in \mathbb{Q}_p$ such that the inequality*

$$|P(w)|_p < H(P)^{-n-\delta}$$

has infinitely many solutions in reducible polynomials $P \in \mathbb{Z}[x]$ with $degP \leqslant n$. Then $\mu(E(\delta)) = 0$.

The proof can be found in [3, 5].

A polynomial $P \in \mathbb{Z}[x]$ with *leading coefficient* a_n will be called *leading* if

$$|a_n| \gg H(P) \quad \text{and} \quad |a_n|_p > p^{-n}. \tag{8}$$

Let $\mathcal{P}_n(H)$ be the set of irreducible primitive leading polynomials $P \in \mathbb{Z}[x]$ of degree n with height $H(P) = H$. Also define

$$\mathcal{P}_n = \bigcup_{H=1}^{\infty} \mathcal{P}_n(H). \tag{9}$$

The reduction to leading polynomials is completed with the help of Lemma 2 and the following lemma.

Lemma 3 *Let $P(x) = a_n x^n + \cdots + a_1 x + a_0$ be an integer polynomial with discriminant $D(P)$ such that $(a_0, a_1, \ldots, a_n) = 1$ and $H(P) \leqslant Q$. Another polynomial $T(x) = b_n x^n + \cdots + b_1 x + b_0$ can be constructed which satisfies the conditions:*

$$H(T) \ll Q, \quad D(T) = D(P), \quad |b_n|_p \gg 1.$$

Proof. To begin we will prove that there exists m_0, $1 \leqslant m_0 \leqslant n+1$, such that

$$\max_{1 \leqslant k \leqslant n+1} |P(k)|_p = |P(m_0)|_p \gg 1.$$

Assume that for some $c_1 = p^d$ the system of inequalities

$$\max_{1 \leqslant k \leqslant n+1} |P(k)|_p < |c_1|_p = p^{-d} \tag{10}$$

holds. The assumptions in the statement of the lemma imply that there exists j_0, $0 \leqslant j_0 \leqslant n$, such that $|a_{j_0}|_p = 1$. Replace system (10) by the system of equations relative to a_i, $0 \leqslant i \leqslant n$, and solve it relatively a_{j_0}. We obtain

$$\begin{cases} \left|a_n + a_{n-1} + \cdots + a_1 + a_0\right|_p = c_1\theta_1, \\ \left|a_n 2^n + a_{n-1} 2^{n-1} + \cdots + a_1 2 + a_0\right|_p = c_1\theta_2, \\ \qquad\qquad \cdots \\ \left|a_n (n+1)^n + a_{n-1}(n+1)^{n-1} + \cdots + a_1(n+1) + a_0\right|_p = c_1\theta_{n+1}, \end{cases} \tag{11}$$

where $\theta_i = p^{d_i}$, $d_i \geqslant 1$ and

$$a_{j_0} = \frac{\Delta_{j_0}}{\Delta}. \tag{12}$$

The determinant Δ in (12) is the Van der Monde determinant:

$$\Delta = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & n+1 \\ & & \ldots & \\ 1 & 2^n & \ldots & (n+1)^n \end{vmatrix} = \prod_{k=0}^{n} k!(n-k)!. \tag{13}$$

The prime number p divides $k!$ with degree at most

$$\left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \cdots \leqslant k \sum_{j=1}^{\infty} p^{-j} \leqslant k,$$

and Δ contains degree at most n^n. For the determinant Δ_{j_0} the inequalities $\Delta_{j_0} = c_1 \Delta'_{j_0}$ and $|\Delta'_{j_0}|_p \leqslant 1$ hold; therefore $|\Delta_{j_0}|_p \leqslant p^{-d}$. Since $|a_{j_0}|_p = 1$ equation (12) gives a contradiction for $d > n^n$.

We denote the roots of P by $\alpha_1, \alpha_2, \ldots, \alpha_n$ and consider the polynomial

$$P_1(x) = P(x + m_0) = a_n x^n + a'_{n-1} x^{n-1} + \cdots + a'_1 x + P(m_0).$$

Its roots are $\beta_j = \alpha_j - m_0$, $1 \leqslant j \leqslant n$, and its discriminant satisfies

$$D(P_1) = a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\beta_i - \beta_j)^2 = a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2 = D(P).$$

The polynomial $T(x) = x^n P_1(\frac{1}{x}) = P(m_0) x^n + a''_{n-1} x^{n-1} + \cdots + a''_1 x + a_n$ has roots $\gamma_j = \frac{1}{\beta_j} = \frac{1}{\alpha_j - m_0}$, $1 \leqslant j \leqslant n$. The absolute value of the discriminant is

$$|D(T)| = P(m_0)^{2n-2} | \prod_{1 \leqslant i < j \leqslant n} (\beta_i - \beta_j)^2 \beta_i^{-2} \beta_j^{-2} |.$$

However, $\prod_{1 \leqslant i < j \leqslant n} \beta_i^{-2} \beta_j^{-2} = (\frac{a_n}{P(m_0)})^{2n-2}$, so that

$$D(T) = a_n^{2n} \prod_{1 \leqslant i < j \leqslant n} (\beta_i - \beta_j)^2 = D(P).$$

The condition $H(T) < c(n)H$ is obviously satisfied as $H(T) = H(P_1)$ and $H(P_1) \asymp H(P)$.

Lemma 4 *Let $\alpha_1, \ldots, \alpha_n$ be the roots of $P \in \mathcal{P}_n$. Then* $\max_{1 \leqslant i \leqslant n} |\alpha_i|_p < p^n$.

For the proof see [11, p85].

For the roots $\alpha_1, \ldots, \alpha_n$ of P we define the sets

$$S(\alpha_i) = \{ w \in \mathbb{Q}_p \ : \ |w - \alpha_i|_p = \min_{1 \leqslant j \leqslant n} |w - \alpha_j|_p \} \ (1 \leqslant i \leqslant n).$$

Let $P \in \mathcal{P}_n$. As α_1 is fixed, we reorder the other roots of P so that $|\alpha_1 - \alpha_2|_p \leqslant |\alpha_1 - \alpha_3|_p \leqslant \cdots \leqslant |\alpha_1 - \alpha_n|_p$. We can assume that there exists a root α_m of P for which $|\alpha_1 - \alpha_m|_p \leqslant 1$ (see [5, p99]. Then we have

$$|\alpha_1 - \alpha_2|_p \leqslant |\alpha_1 - \alpha_3|_p \leqslant \cdots \leqslant |\alpha_1 - \alpha_m|_p \leqslant 1 \leqslant \cdots \leqslant |\alpha_1 - \alpha_n|_p. \tag{14}$$

Let $\varepsilon > 0$ be sufficiently small, $d > 0$ be a large fixed number, $\varepsilon_1 = \frac{\varepsilon}{d}$, and $T = [\varepsilon_1^{-1}] + 1$. We define real numbers μ_j and integers l_j by the relations

$$|\alpha_1 - \alpha_j|_p = H^{-\mu_j}, \ \frac{l_j}{T} \leqslant \mu_j < \frac{l_j + 1}{T} \ (2 \leqslant j \leqslant m). \tag{15}$$

It follows from (14) and (15) that $\mu_2 \geqslant \mu_3 \geqslant \dots \geqslant \mu_m \geqslant 0$ and $l_2 \geqslant l_3 \geqslant \dots \geqslant l_m \geqslant 0$. We assume that $\mu = 0$ and $l_j = 0$ if $m < j \leqslant n$.

Now, for every polynomial $P \in \mathcal{P}_n(H)$ we define a non–negative vector $\bar{l} = (l_2, \dots, l_n)$. In [5, p99–100] it is shown that the number of such vectors is finite and depends on n, p and T only. All polynomials $P \in \mathcal{P}_n(H)$ corresponding to the same vector $\bar{l}$ are grouped together into a class $\mathcal{P}_n(H, \bar{l})$. We define

$$\mathcal{P}_n(\bar{l}) = \bigcup_{H=1}^{\infty} \mathcal{P}_n(H, \bar{l}). \tag{16}$$

Let $K_0 = \{w \in \mathbb{Q}_p : |w|_p < p^n\}$ be the disc of radius p^n centered at 0. Define

$$p_j = p_j(P) = \frac{l_{j+1} + \dots + l_n}{T} \quad (1 \leqslant j \leqslant n-1).$$

Lemma 5 *Let $w \in S(\alpha_1)$ and $P \in \mathcal{P}_n(H)$. Then*

$$H^{-p_1} \ll |P'(\alpha_1)|_p \ll H^{-p_1+(m-1)\varepsilon_1},$$

$$|P^{(j)}(\alpha_1)|_p \ll H^{-p_j+(m-j)\varepsilon_1} \quad \textit{for} \;\; 2 \leqslant j \leqslant m,$$

and

$$|P^{(j)}(\alpha_1)|_p \ll 1 \quad \textit{for} \;\; m < j \leqslant n.$$

Proof. From Lemma 4 we have $p^{-n} < |H|_p \leqslant 1$. Then, after differentiating j times $P(w) = H(w - \alpha_1)\dots(w - \alpha_n)$ $(1 \leqslant j \leqslant n)$ and using (14) and (15) the lemma is proved.

Lemma 6 *Let $\delta, \sigma \in \mathbb{R}_+$. Further, let $P, Q \in \mathbb{Z}[x]$ be two relatively prime polynomials of degree at most n with* $\max(H(P), H(Q)) \leqslant H$ *and $H > H_0(\delta)$. Let $K(\alpha, H^{-\eta})$ be a disc of radius $H^{-\eta}$ centred at α. If there exists a number $\tau > 0$ such that for all $w \in K(\alpha, H^{-\eta})$,*

$$\max(|P(w)|_p, |Q(w)|_p) < H^{-\tau},$$

then

$$\tau + 2max(\tau - \eta, 0) < 2n + \delta.$$

For the proof see [4, Lemma 5].

Lemma 7 (Hensel) *Let $P \in \mathbb{Z}_p[x]$, $\xi = \xi_0 \in \mathbb{Z}_p$ and $|P(\xi)|_p < |P'(\xi)|_p^2$. Then, for $n \to \infty$ the sequence*

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

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

$$|\alpha - \xi|_p \leqslant \frac{|P(\xi_n)|_p}{|P'(\xi_n)|_p^2}.$$

For the proof see [3, p134].

Lemma 8 *For any $Q > 1$, $w \in \mathbb{Q}_p$, $v \in [0, \frac{1}{2}]$ and $c_1c_2 > p^3$ the system of inequalities*

$$\begin{cases} |P(w)|_p < c_1 Q^{-n-1+v}, \\ |P'(w)|_p < c_2 Q^{-v}, \end{cases}$$

has solutions in integer polynomials P with $H(P) < Q$.

Proof. We will use Dirichlet's pigeonhole principle. First, choose positive integer l_1 and l_2 such that

$$p^{l_1+l_2} < Q^{n+1} \leqslant p^{l_1+l_2+1}. \tag{17}$$

The number of possible values of $P(w) = a_1 + a_1 p + \cdots + a_k p^k + \ldots$ which have different vectors $\bar{a} = (a_0, a_1, \ldots, a_{l_1-1})$ is p^{l_1}. Similarly, the number of possible values of $P'(w) = b_1 + b_1 p + \cdots + b_s p^s + \ldots$ with different vectors $\bar{b} = (b_0, b_1, \ldots, b_{l_2-1})$ is p^{l_2}. The number of polynomials $P(x) = d_n x^n + a_{n-1} x^{n-1} + \cdots + d_1 x + d_0$ for $0 \leqslant d_i \leqslant Q$ is at least Q^{n+1}. Therefore, for $Q^{n+1} > p^{l_1+l_2}$ there are at least two polynomials P_1 and P_2 which have the same vectors $\bar{a}$ and $\bar{b}$. Let $R(x) = P_1(x) - P_2(x)$. It is clear that $H(R) \leqslant Q$. Now, for fixed c_1, c_2 and v choose l_1 and l_2 such that

$$\begin{cases} p^{l_1-1} \leqslant c_1^{-1} Q^{n+1-v} < p^{l_1}, \\ p^{l_2-1} \leqslant c_2^{-1} Q^{v} < p^{l_2}. \end{cases} \tag{18}$$

Since $|R(w)|_p \leqslant p^{-l_1}$ and $|R'(w)|_p \leqslant p^{-l_2}$ these inequalities imply that

$$|R(w)|_p \leqslant p^{-l_1} < c_1 Q^{-n-1+v},$$

and

$$|R'(w)|_p \leqslant p^{-l_2} < c_1 Q^{-v}.$$

Inequalities (18) together with (17) hold for $c_1c_2 > p^3$ which completes the proof.

Proof of Theorem 1 modulo Theorem 2.

We will now show that Theorem 1 follows from Theorem 2. Let $w_1 \in B_1 = K \setminus M_{n,Q}(c_1, c_2)$ such that $\mu(B_1) \geqslant \frac{\mu(K)}{2}$. Assume that $\gamma = p^{-6} 2^{-n-9}$. Then, there exists a polynomial $P_1 \in (P)_n(Q)$ such that the following system of inequalities

$$\begin{cases} \gamma Q^{-n-1+v} \leqslant |P_1(w_1)|_p < Q^{-n-1+v}, \\ \gamma Q^{-v} \leqslant |P_1'(w_1)|_p < p^3 Q^{-v} \end{cases} \tag{19}$$

holds. The upper bounds follow from Lemma 8. If the first condition of (19) does not hold then $|P_1(w_1)|_p < \gamma Q^{-n-1+v}$ and $|P_1'(w_1)|_p < p^3 Q^{-v}$. This implies that w_1 belongs to a set with measure at most $\frac{\mu(K)}{4}$. If the second condition of (19) does not hold then w_1 also belongs to a set with measure at most $\frac{\mu(K)}{4}$. This contradicts the choice of w_1.

Let $w \in K_1$ where K_1 is the disc $\{w \in \mathbb{Q}_p : |w - w_1|_p < Q^{-\frac{3}{4}}\}$ and obtain the Taylor representation of $P_1'(w)$ on this disc so that

$$P_1'(w) = P_1'(w_1) + \sum_{i=2}^{n}((i-1)!)^{-1}P_1^{(i)}(w_1)(w - w_1)^{i-1}.$$

Since

$$|(i-1)!|_p^{-1}|P_1^{(i)}(w_1)|_p|w - w_1|_p^{i-1} \ll Q^{-\frac{3}{4}},$$

and

$$|P_1'(w)|_p \geqslant \gamma Q^{-v} \gg Q^{-\frac{1}{2}},$$

for all $w \in K_1$ we obtain that $|P_1'(w)|_p = |P_1'(w_1)|_p$. Let α_1 be the closest root of $P_1(w)$ to the point w_1. From Lemma 1

$$|w_1 - \alpha|_p \leqslant |P_1(w_1)|_p|P_1'(w_1)|_p^{-1} \leqslant \gamma^{-1}Q^{-n-1+2v}. \tag{20}$$

To estimate the distance between w_1 and the root of the polynomial we can also apply Lemma 7. Since $|P_1(w_1)|_p < |P_1'(w_1)|_p^2$ we obtain that the sequence in Lemma 7 converges to the root $\alpha_1 \in \mathbb{Q}_p$ and

$$|w_1 - \alpha_1|_p \leqslant |P_1(w_1)|_p|P_1'(w_1)|_p^{-2} \leqslant \gamma^{-2}Q^{-n-1+3v}. \tag{21}$$

Since $0 < \gamma < 1$ and $v > 0$ the right part of (20) is greater then the right part of (21). That imply the root α belongs to the disc with center w_1 of radius less than the radius for the disc defined for the root α_1. From Lemma 7 we find that $\alpha_1 \in \mathbb{Q}_p$ but Lemma 1 does not guarantee that $\alpha \in \mathbb{Q}_p$. Suppose that $\alpha \neq \alpha_1$ and consider the discriminant of the polynomial $P \in \mathcal{P}_n(Q)$

$$D(P) = a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2. \tag{22}$$

Lemma 4 implies that $|\alpha_i - \alpha_j|_p \ll 1$. The product in(22) contains the difference $(\alpha - \alpha_1)$ for some $i \neq j$. We have $D(P) \in \mathbb{Z}$ and $|D(P)| \ll Q^{2n-2}$; therefore $|D(P)|_p \gg Q^{-2n+2}$. From (20) and (21) we further obtain that

$$|\alpha_1 - \alpha|_p = |\alpha_1 - w_1 + w_1 - \alpha|_p \leqslant \max\{|w_1 - \alpha_1|_p, |w_1 - \alpha|_p\} \leqslant \gamma^{-2}Q^{-n-1+3v}.$$

Therefore

$$Q^{-2n+2} \ll |D(P)|_p \ll |\alpha_1 - \alpha|_p^2 < \gamma^{-4}Q^{-2n-2+6v}. \tag{23}$$

For $v \leqslant \frac{1}{2}$ and $Q > Q_0$ the inequality $Q^{-2n+2} \ll \gamma^{-4}Q^{-2n-2+6v}$ is a contradiction. Hence, $\alpha_1 = \alpha$. Thus, $\alpha \in \mathbb{Q}_p$ and $|w_1 - \alpha|_p$ satisfies condition (20).

From the representation of $P'(\alpha)$ as a Taylor series

$$P_1'(\alpha) = P_1'(w_1) + \sum_{i=2}^{n}((i-1)!)^{-1}P^{(i)}(w_1)(\alpha - w_1)^{i-1}, \tag{24}$$

the estimate

$$|(i-1)!|_p^{-1}|P^{(i)}(w_1)|_p|\alpha-w_1|_p^{i-1} \ll Q^{-n-1+2v}$$

and condition (20) we obtain

$$|P_1'(\alpha)|_p = |P_1'(w_1)|_p < p^3Q^{-v}.$$

Therefore

$$|D(P)|_p = |a_n^2\prod_{k=2}^{n}(\alpha_1-\alpha_k)^2|_p|a_n^{2n-4}\prod_{2\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)^2|_p \ll |P'(\alpha)|_p^2 \ll Q^{-2v}. \tag{25}$$

Inequality (20) implies that in the neighbourhood of the point $w_1 \in B_1$ there exists a root α of the polynomial P_1 with discriminant satisfying (25).

Further, let $w_2 \in B_1$ and construct a polynomial P_2 such that its discriminant satisfies (25). If $|w_1-w_2|_p > \gamma^{-1}Q^{-n-1+2v}$ then the polynomials $P_1(w)$ and $P_2(w)$ are different. From the Taylor expansion of P_1 at the point $w = w_2$ we obtain

$$P_1(w_2) = P_1(w_1) + P_1'(w_1)(w_2-w_1) + \sum_{i=2}^{n}(i!)^{-1}P^{(i)}(w_1)(w_2-w_1)^i. \tag{26}$$

Since

$$|i!|_p^{-1}|P^{(i)}(w_1)|_p|w_2-w_1|_p^i \ll Q^{-2n},\ i \geqslant 2,$$

$$|P_1'(w_1)|_p|w_2-w_1|_p > \gamma Q^{-v}\gamma^{-1}Q^{-n-1+2v} = Q^{-n-1+v},$$

and

$$|P_1(w_1)|_p < Q^{-n-1+v},$$

we can obtain from (26) that

$$|P_1(w_2)|_p > Q^{-n-1+v}.$$

By construction $|P_1(w_2)|_p < Q^{-n-1+v}$ which proves that $P_2(w) \neq P_1(w_1)$. Repeating the described procedure several times, excluding at each step the disk $K(w_i, c(n)Q^{-n-1+2v})$, we can construct $k \geqslant Q^{n+1-2v}$ points w_i and polynomials P_i corresponding to them, such that

$$|D(P_i)|_p < Q^{-2v}.$$

Proof of Theorem 2.

From Lemma 8 for $c_1 = 1$, $c_2 = p^3$, $Q > 1$ and arbitrary $w \in \mathbb{Q}_p$ the system

$$\begin{cases} |P(w)|_p < Q^{-n-1+v}, \\ |P'(w)|_p < p^3Q^{-v}, \end{cases} \tag{27}$$

holds for some polynomial P with $H(P) \leqslant Q$.

Denote by $M_1(c_3, c_4)$ the set of w for which the system of inequalities

$$\begin{cases} |P(w)|_p < c_3 Q^{-n-1+v}, \\ Q^{-\frac{2}{3}} \leqslant |P'(w)|_p < c_4 p^3 Q^{-v}, \end{cases} \tag{28}$$

always has solutions in polynomials $P \in \mathcal{P}_n(Q)$. We again use the Taylor expansion of $P'(w)$ in the disc $\{w \in \mathbb{Q}_p : |w - \alpha|_p < Q^{-\frac{3}{4}}\}$, where α is the closest root to w. We have

$$P'(w) = P'(\alpha) + \sum_{j=2}^{n} ((j-1)!)^{-1} P^{(j)}(\alpha)(w-\alpha)^{j-1}, \tag{29}$$

For any j, $2 \leqslant j \leqslant n$, we have

$$|(j-1)!|_p^{-1} |P^{(j)}(\alpha)|_p |w-\alpha|_p^{j-1} \ll Q^{-3/4}, \tag{30}$$

therefore from (29) and (30) it follows that $|P'(\alpha)|_p = |P'(w)|_p$ and the system of inequalities (27) can be rewritten as

$$\begin{cases} |P(w)|_p < c_3 Q^{-n-1+v}, \\ Q^{-\frac{2}{3}} < |P'(\alpha)|_p < c_4 p^3 Q^{-v}. \end{cases} \tag{31}$$

Now we prove that $\mu(M_1(c_3, c_4)) \leqslant \frac{\mu(K)}{8}$. By Lemma 1 and (31) we have

$$|w - \alpha|_p < c_3 Q^{-n-1+v} |P'(\alpha)|_p^{-1}. \tag{32}$$

Let $\sigma_1(P)$ denote the set of solutions of inequality (32). We introduce the disc $\sigma_2(P)$

$$\sigma_2(P) := \{w \in \mathbb{Q}_p : |w - \alpha|_p < c_5 Q^{-2+v} |P'(\alpha)|_p^{-1}\}, \tag{33}$$

where the value c_5 will be specified later. Obviously

$$\mu(\sigma_1(P)) < c_3 c_5^{-1} Q^{-n+1} \mu(\sigma_2(P)). \tag{34}$$

Fix the vector $\bar{b} = (a_n, \ldots, a_2)$ of coefficients of P. All polynomials with the same vector $\bar{b}$ form the class $\mathcal{P}(\bar{b})$. Thus we divide $\mathcal{P}_n(Q)$ into classes according to the vector $\bar{b}$.

The disc $\sigma_2(P_1)$, $P_1 \in \mathcal{P}(\bar{b})$, is called *essential* if for any $P_2 \in \mathcal{P}(\bar{b})$

$$\sigma_2(P_1) \cap \sigma_2(P_2) = \emptyset \tag{35}$$

holds. The disc $\sigma_2(P_1)$, $P_1 \in \mathcal{P}(\bar{b})$, is called *inessential* otherwise; i.e. if it intersects another disc $\sigma_2(P_2)$ with $P_2 \in \mathcal{P}(\bar{b})$.

a) The case of essential discs. In this case every point $w \in K$ belongs to at most one essential disc $\sigma_2(P)$. Therefore for any vector $\bar{b}$

$$\sum_{P \in \mathcal{P}_1(\bar{b})} \mu(\sigma_2(P)) \leqslant \mu(K). \tag{36}$$

The number of different vectors in the class $\mathcal{P}(\bar{b})$ is at most $(2Q+1)^{n-1} < 2^n Q^{n-1}$ for $Q > Q_0$. Therefore

$$\sum_{\bar{b}} \sum_{P \in \mathcal{P}(\bar{b})} \mu(\sigma_1(P)) < c_1 c_5^{-1} 2^n \mu(K). \tag{37}$$

For $c_5 = 2^{n+3} c_3$ the estimate in (37) is at most $\frac{\mu(K)}{8}$.

b) The case of inessential discs. We will first estimate the values of $|P_j(w)|_p$, $j = 1, 2$, on the intersection $\sigma_2(P_1, P_2)$ of the discs $\sigma_2(P_1)$ and $\sigma_2(P_2)$. From the Taylor expansion of P_j on the disc $\sigma_2(P_j)$ in the neighborhood of the root $\alpha = \alpha(P_j)$ we obtain

$$P_j(w) = P_j'(\alpha)(w - \alpha) + \sum_{i=2}^{n} (i!)^{-1} P_j^{(i)}(\alpha)(w - \alpha)^i. \tag{38}$$

From (33) we further obtain that

$$|P_j'(\alpha)|_p |w - \alpha|_p < c_5 Q^{-2+v}, \tag{39}$$

and for $i \geqslant 2$ from the lower bound for $|P'(\alpha)|_p$ in (31) we have

$$|i!|_p^{-1} |P^{(i)}(\alpha)|_p |w - \alpha|_p^i \ll Q^{-4+2v+\frac{4}{3}} < c_5 Q^{-2+v} \tag{40}$$

for $v \in [0, \frac{1}{2}]$ and $Q > Q_0$. The expansion (38), together with (39) and (40) imply that

$$|P_j(w)|_p < c_5 Q^{-2+v} \tag{41}$$

Similarly, by the Taylor representation of P_j' on the disc $\sigma_2(P_j)$ in the neighbourhood of the root $\alpha = \alpha(P_j)$ we have

$$P_j'(w) = P_j'(\alpha) + \sum_{i=2}^{n} (i!)^{-1} P_j^{(i)}(\alpha)(w - \alpha)^{i-1}.$$

The second inequality in (31) and the estimate

$$|i!|_p^{-1} |P^{(i)}(\alpha)|_p |w - \alpha|_p^{i-1} \ll c_5 Q^{(i-1)(-2+v+\frac{2}{3})}, \quad i \geqslant 2$$

imply that

$$|P_j'(w)|_p < c_4 p^3 Q^{-v}.$$

Denote the difference between P_1 and P_2 by $R(x) = P_2(x) - P_1(x)$. Since P_1 and P_2 belong to the same class $\mathcal{P}(\bar{b})$ we know that R is linear, so that $R(x) = ax + b$ for some a, b. Also, (41) and the estimate for the derivative imply that

$$\begin{cases} |aw + b|_p < c_5 Q^{-2+v}, \\ |R'(w)|_p = |a|_p < c_4 p^3 Q^{-v}, \\ \max\{|a|, |b|\} \leqslant Q. \end{cases} \tag{42}$$

From the first two of these inequalities it follows that $|b|_p < c_4 p^3 Q^{-v}$ which further implies that for fixed a the number b can have at most $2a\mu(K)$ values. The value a has at most $2c_4 p^3 Q^{1-v}$ values. As a result, the measure of the set of w satisfying (42) does not exceed $4c_4 c_5 p^3 \mu(K) = 2^{n+5} c_3 c_4 p^3 \mu(K)$. Then, for $c_3 c_4 < p^{-3} 2^{-n-8}$, this estimate is not greater than $\frac{\mu(K)}{8}$.

Thus, the total measure for the essential and inessential discs is at most $\frac{\mu(K)}{4}$.

Our next task is to estimate the measure of $M''_n(v)$ which we define to be the set of w for which the system

$$\begin{cases} |P(w)|_p < Q^{-n-1+v} \\ |P'(w)|_p < Q^{-v_1} \\ |a_j| \leqslant Q, \ 0 \leqslant j \leqslant n, \end{cases} \tag{43}$$

has solutions. We will show that $\mu(M''_n(v)) < \frac{\mu(K)}{4}$.

Four different cases will be considered according to the value of $l_2 T^{-1} + p_1$.

Case 1.

$$l_2 T^{-1} + p_1 \geqslant n + 1 - v. \tag{44}$$

Let $\mathcal{P}_t(\bar{l})$ be the set $\{P \in \mathcal{P}_n(H, \bar{l}) \mid 2^t \leqslant H < 2^{t+1}\}$. Since Q is sufficiently large and $H \leqslant Q$, we may assume that $t_0 < t \ll \log Q$. Let $w \in S(\alpha_1)$, then

$$|w - \alpha_1|_p \leqslant 2^{t(-n-1+v+p_1+(n-1)\varepsilon)} \tag{45}$$

or

$$|w - \alpha_1|_p \leqslant 2^{\frac{t}{2}(-n-1+v+p_2+(n-2)\varepsilon)}. \tag{46}$$

Simple calculations show that for this case the second inequality is better. For all the other cases we shall use the first one. Divide the disc K into smaller discs K_j of radius $2^{-(\frac{n+1-v-p_2}{2}-\gamma)}$, where γ is a positive constant and will be specified below.

For an integer polynomial P and a disk K_j we shall use the definition that "$P(w)$ belongs to K_j" or "K_j contains $P(w)$", if there is a point $w \in K_j$, that satisfies the system (43). Let $\sigma(P)$ denote the set of w that satisfy (43).

a) Assume that at most one polynomial $P \in \mathcal{P}_t(\bar{l})$ belongs to every K_j. Then for every polynomial the measure of those w which satisfy (43) is at most $c(n) 2^{-t(\frac{n+1-v-p_2-(n-2)\varepsilon}{2})}$. The number of K_j is less than $2^{t(\frac{n+1-v-p_2}{2}-\gamma)}\mu(K)$. Therefore

$$\sum_{P \in \mathcal{P}_t(\bar{l})} \mu(\sigma(P)) \ll \sum_{P \in \mathcal{P}_t(\bar{l})} 2^{t(\frac{n+1-v-p_2}{2}-\gamma)} \mu(K) c(n) 2^{-t(\frac{n+1-v-p_2-(n-2)\varepsilon}{2})} \ll 2^{-t\gamma_1}, \tag{47}$$

where $\gamma_1 = \gamma - \frac{n-2}{2}\varepsilon$.

Sum (47) over all $t \geqslant t_0$. Since $\sum_{t > t_0} 2^{-t\gamma_1} \ll 2^{-t_0 \gamma_1}$ for sufficiently large t_0 the measure of those w such that (43) holds with polynomials P satisfying case 1 a), does not exceed $\frac{\mu(K)}{32}$.

b) Now assume the contrary: that there are discs K_j, that contain at least two polynomials, i.e. we can find polynomials P_1 and P_2 in $\mathcal{P}_t(\bar{l})$, points w_1 and w_2 in K_j, such that the system of inequalities

$$\begin{cases} |P_1(w_1)|_p \ll 2^{t(-n-1+v)}, \\ |P_1'(x_1)|_p \ll 2^{-tv_1}, \\ |P_2(x_2)|_p \ll 2^{t(-n-1+v)}, \\ |P_2'(x_2)|_p \ll 2^{-tv_1}. \end{cases}$$

holds. We will now estimate the values of $|P_1(w)|_p$ and $|P_2(w)|_p$ for $w \in K_j$. Using Taylor's expansion for P_i at the point α_1 we have

$$P_i(w) = \sum_{j=1}^{n} (j!)^{-1} P_i^{(j)}(\alpha_1) \cdot (w - \alpha_1)^j, \ i = 1, 2.$$

Using estimates for $|P^{(j)}(\alpha_1)|_p$ from Lemmas 1 and 5 we therefore have

$$|P_i(x)|_p = |\sum_{j=1}^{n} (j!)^{-1} P_i^{(j)}(\alpha_1) \cdot (w - \alpha_1)^j|_p \ll$$

$$\ll \max_{1 \leqslant j \leqslant n} 2^{-tp_j} 2^{tj(\frac{-n+v-1+p_j+(n-j)\varepsilon}{j}+\gamma)} \ll 2^{t(-n-1+v+n\gamma_1)}.$$

For polynomials P_1 and P_2 with no common roots we can apply Lemma 6 with $\tau = 1 + n - v - n\gamma_1$ and $\eta = \frac{n+1-v-p_2}{2} - \gamma$. It is necessary to check whether $\tau + 2\max(\tau - \sigma, 0) < 2n + \delta$ for any $\delta > 0$. We have

$$3 + 3n - 3v - 3n\gamma_1 - n - 1 + v + p_2 + 2\gamma < 2n + \delta.$$

Hence, it follows that

$$2 - 2v + p_2 < \delta + (3n - 2)\gamma_1.$$

However, $2 - 2v > \delta + (3n-2)\gamma_1$ for $v \leqslant \frac{1}{2}$ and sufficiently small δ which leads to a contradiction.

Case 2.

$$n + 0.1 \leqslant l_2 T^{-1} + p_1 < n + 1 - v. \tag{48}$$

Again, divide the disc K into smaller discs K_j, with radius $2^{t(-\frac{l_2}{T}+\gamma)}$.

a) Assume that at most one polynomial $P \in \mathcal{P}_t(\bar{l})$ belongs to every K_j. From (45) for every polynomial the measure of those w which satisfy (43), does not exceed $c(n)2^{-t(n+1-v-p_1-(n-1)\varepsilon)}$. The number of K_j is less than $2^{t(n+1-v-p_1-\gamma)}\mu(K)$. Therefore

$$\sum_{P \in \mathcal{P}_t(\bar{l})} \mu(\sigma(P)) \ll \sum_{P \in \mathcal{P}_t(\bar{l})} 2^{t(\frac{l_2}{T}-\gamma)} 2^{-t(n+1-v-p_1-(n-1)\varepsilon)} \ll 2^{-t\gamma_2}, \tag{49}$$

where $\gamma_2 = \gamma - (n-1)\varepsilon$. Again we sum the estimate (49) over all $t > t_0$. And similarly as the argument following (47) we obtain an estimate less than $\frac{\mu(K)}{32}$.

b) As in Case 1, now assume the existence of a disc K_j that contains at least two different polynomials P_1 and P_2. For any $w \in K_j$ by Taylor's expansion we get

$$|P_i(w)|_p \ll 2^{-t(l_2T^{-1}+p_1-n\gamma)},\ i=1,2.$$

For P_1 and P_2 having no common roots in K_j we apply Lemma 6 with $\tau = l_2T^{-1} + p_1 - n\gamma$ and $\eta = l_2T^{-1} - \gamma$. Note that $l_2T^{-1} \leqslant p_1$. Then

$$3l_2T^{-1} + 3p_1 - 3n\gamma - 2l_2T^{-1} + 2\gamma < 2n + \delta$$

and

$$3p_1 + l_2T^{-1} - (3n-2)\gamma < 2n + \delta.$$

However,

$$3p_1 + l_2T^{-1} - (3n-2)\gamma \geqslant 2p_1 + 2l_2T^{-1} - (3n-2)\gamma > 2n + 0.2 - (3n-2)\gamma > 2n + \delta$$

for sufficiently small δ and γ. Again there is a contradiction.

Case 3.

$$\frac{7}{4} \leqslant l_2T^{-1} + p_1 < n + 0.1. \qquad (50)$$

This case covers the widest range of values for $l_2T^{-1} + p_1$ and is the most difficult one. We again divide the disc K into smaller discs K_j of radius $2^{-tl_2T^{-1}}$. We need to estimate the value of a polynomial $P \in \mathcal{P}_n$ and its derivative for $w \in K_j$. For this purpose we rewrite $P(w)$ using the Taylor formula in the neighbourhood of the point α_1

$$\begin{aligned}
P(w) &= P'(\alpha_1)(w-\alpha_1) + \sum_{i=2}^{n}(i!)^{-1}P^{(i)}(\alpha_1)\cdot(x-\alpha_1)^i,\\
|P'(\alpha_1)|_p|w-\alpha_1|_p &\ll 2^{t(-l_2T^{-1}-p_1)},\\
|2|_p^{-1}|P''(\alpha_1)|_p|w-\alpha_1|_p^2 &\ll 2^{t(-p_2-2l_2T^{-1})} \ll 2^{-t(l_2T^{-1}+p_1)},\\
|i!|_p^{-1}|P^{(i)}(\alpha_1)|_p|w-\alpha_1|_p^i &\ll 2^{t(-p_i-il_2T^{-1})} \ll 2^{-t(l_2T^{-1}+p_1)},\ i \geqslant 3,\\
|P(w)|_p &\ll 2^{-t(l_2T^{-1}+p_1)}. \qquad (51)
\end{aligned}$$

Similarly from the expansion of $P'(w)$ on the disc K_j we obtain

$$\begin{aligned}
P'(w) &= P'(\alpha_1) + \sum_{i=2}^{n}((i-1)!)^{-1}P^{(i)}(\alpha_1)\cdot(x-\alpha_1)^{i-1},\\
|P'(\alpha_1)|_p &\asymp 2^{-tp_1},\\
|(i-1)!|_p^{-1}|P^{(i)}(\alpha_1)|_p|w-\alpha_1|_p^{i-1} &\ll 2^{t(-p_i-(i-1)l_2T^{-1})} \ll 2^{-tp_1},\ i \geqslant 2,\\
|P'(w)|_p &\ll 2^{-tp_1}. \qquad (52)
\end{aligned}$$

Thus if P belongs to the disc K_j then for $w \in K_j$ the inequalities

$$\begin{cases} |P(w)|_p \ll 2^{-t(p_1+l_2t^{-1})}, \\ |P'(w)|_p \asymp 2^{-tp_1} \end{cases} \tag{53}$$

hold.

For some $\theta \geqslant 0$ we assume that the disc K_j contains $c(n)2^{t\theta}$ polynomials. Then by Lemma 1 the measure of $w \in K$, that satisfy (43) does not exceed

$$c(n)2^{t(-n+v-1+p_1)}2^{t\theta}2^{tl_2T^{-1}} = m(t). \tag{54}$$

For $\theta < n+1-v-l_2T^{-1}-p_1$ the series $\sum_{t=1}^{\infty} m(t)$ converges. Therefore for $t > t_0$ we obtain the estimate $\sum_{t>t_0} m(t) < \frac{\mu(K)}{32}$.

We introduce

$$u = n+1-v-p_1-l_2T^{-1}.$$

From (50) and $v \leqslant 0.5$ it follows that $u \geqslant 0.4$. In what follows let $u_1 = u - 0.2 \geqslant 0.2$ and write u_1 as $u_1 = [u_1] + \{u_1\}$, where [ ] and { } denote the integer and fractional parts respectively.

Let $\theta \geqslant u$. By Dirichlet's principle we have that there are at least $c(n)2^{t(\{u_1\}+0.2)}$ polynomials $P_1, P_2, \ldots, P_k$, with $k \gg 2^{t(\{u_1\}+0.2)}$, which have the same first $[u_1]$ coefficients.

Consider the polynomials $R_j(w) = P_{j+1}(w) - P_1(w)$, $j \geqslant 1$, which satisfy:

$$\begin{aligned} \deg R_j(w) &\leqslant n-[u_1] = l_2T^{-1}+p_1+v+\{u_1\}-0.8, \\ H(R_j) &\leqslant 2^{t+2}. \end{aligned} \tag{55}$$

From (53) we get

$$\begin{cases} |R_j(w)|_p \ll 2^{-t(p_1+l_2T^{-1})}, \\ |R_j'(w)|_p \ll 2^{-tp_1}, \ i=1,\ldots,k. \end{cases} \tag{56}$$

Every coefficient $a_j(R)$, $1 \leqslant j \leqslant n-[u_1]$ of the polynomial R_j lies in $[-2^{t+1}; 2^{t+1}]$. For each coefficient divide this interval into smaller intervals of length $2^{t\mu}$, where $\mu = 1 - \frac{\{u_1\}}{n-[u_1]}$. Then, at least $c(n)2^{0.2t}$ polynomials have their lying in the same intervals. Hence the first $u-[u_1]$ coefficients of the polynomials $S_j(w) = R_{j+1}(w) - R_j(w)$ are at most $c(n)2^{t\mu}$. For these polynomials S_j we obtain a similar system of inequalities to (56); namely

$$\begin{cases} |S_i(w)|_p \ll 2^{-t(l_2 \cdot T^{-1}+p_1)}, \\ |S_i'(w)|_p \ll 2^{-tp_1}, \\ \deg S_i(w) \leqslant n-[u_1], \\ H(S_i) < 2^{t\mu}, \ 1 \leqslant i \leqslant k-1. \end{cases} \tag{57}$$

a) Suppose that amongs the polynomials S_j there are two which are coprime. Then we apply Lemma 6 on the disc K_j with $\tau = p_1 + l_2 \cdot T^{-1}$ and $\eta = l_2T^{-1}$ to get

$$\begin{aligned} l_2T^{-1}+3p_1 &< 2(n-[u_1])(1-\frac{\{u_1\}}{n-[u_1]})+\delta_1 \\ &= 2(n-u_1)+\delta_1 = 2p_1+2l_2T^{-1}+2v-1.6+\delta_1, \ \delta_1 < \delta. \end{aligned} \tag{58}$$

Since $l_2T^{-1} \leqslant p_1$ and $v \leqslant \frac{1}{2}$ we have a contradiction for $\delta < 0.6$.

b) If all polynomials S_j can be written lS_0 for some polynomial S_0 then there exists $l > \frac{k}{3}$ such that $(l,p) = 1$. Obviously the height of the polynomial $H(S_0) \ll 2^{-0.2t}H(S_i) \ll 2^{t(0.8-\frac{\{u_1\}}{n-[u_1]})}$. In the first inequality of (57) assume that $i = 0$, and on the RHS pass to the height $H(S_0)$ to obtain the inequality

$$|S_0(w)|_p \ll 2^{-t(l_2T^{-1}+p_1)(0.8-\frac{\{u_1\}}{n-[u_1]})^{-1}}. \tag{59}$$

If now the inequality

$$p_1 + l_2 \cdot T^{-1} > (n - [u_1] + 1)(0.8 - \frac{\{u_1\}}{n - [u_1]}) \tag{60}$$

holds, then by Sprindzuk's theorem, see [11], the inequality (59) holds for a set of $w \in \mathbb{Q}_p$ with measure tending to zero for $t > t_0$ and $t_0 \to \infty$. Condition (50) implies that (60) is true. Therefore, for appropriate t_0 this measure can be bounded above by $\frac{\mu(K)}{32}$.

c) If there are reducible polynomials among the S_i then we use Lemma 2. We again check the inequality

$$l_2 \cdot T^{-1} + p_1 > (n - [u_1])(1 - \frac{\{u_1\}}{n - [u_1]}) = n - u_1 = l_2 \cdot T^{-1} + p_1 + v - 0.8.$$

It obviously holds for $v \leqslant 0.5$. Thus the measure of those $w \in \mathbb{Q}_p$ for which the system (57) holds for these polynomials does not exceed $\frac{\mu(K)}{32}$.

Case 4.

$$l_2T^{-1} + p_1 < \frac{7}{4}. \tag{61}$$

We will estimate the expression $l_2T^{-1}+p_1$ from below. To do this we have to prove that $|P'(w)|_p = |P'(\alpha)|_p \asymp 2^{-tp_1}$. From (43) we have that $|P'(w)|_p \ll 2^{-\frac{2t}{3}}$, therefore $p_1 \geqslant \frac{2}{3}$. Thus we need to consider the system

$$\begin{cases} |P(w)|_p < 2^{t(-n-1+v)}, \\ |P'(w)|_p < 2^{-2t/3}, \\ \frac{2}{3} < l_2T^{-1} + p_1 < \frac{7}{4}. \end{cases} \tag{62}$$

Let α_1 be the closest root to w and introduce the discs $\sigma(P)$ and $\sigma_1(P)$ given by

$$\sigma(P) = \{w \in K \ : \ |w - \alpha_1|_p < 2^{t(-n-1+v)}|P'(\alpha_1)|_p^{-1}\}. \tag{63}$$

$$\sigma_1(P) = \{w \in K : \ |w - \alpha_1|_p < 2^{-t}|P'(\alpha_1)|_p^{-1}\}. \tag{64}$$

From (63) and (64) we get

$$\mu(\sigma(P)) \ll 2^{-t(n-v)}\mu(\sigma_1(P)). \tag{65}$$

Fix a vector $\bar{b} = (a_n, a_{n-1}, \ldots, a_2)$, where a_j, $0 \leqslant j \leqslant n$, are the coefficients of the polynomial P. The set of polynomials with vector $\bar{b}$ is denoted by $\mathcal{P}_{\bar{b}}$. Obviously $\#\mathcal{P}_{\bar{b}} \asymp 2^{t(n-1)}$.

a) First, we consider polynomials P_1 such that $\sigma_1(P_1) \bigcap \sigma_1(P_2) = \emptyset$ for any $P_2 \in \mathcal{P}_{\bar{b}}$. Then $\sum_{P_1 \in \mathcal{P}_{\bar{b}}} \mu(\sigma_1(P_1)) < \mu(K)$. Inequality (65) implies that

$$\sum_{\bar{b}} \sum_{P \in \mathcal{P}_{\bar{b}}} \mu(\sigma P) \ll 2^{t(v-1)}.$$

Since $v-1 < 0$ the series $\sum_{t=1}^{\infty} 2^{t(v-1)}$ converges and its sum $\sum_{t>t_0} 2^{t(v-1)}$ for appropriate t_0 will be less than $\frac{\mu(K)}{32}$.

b) If there exists $P_2 \in \mathcal{P}_{\bar{b}}$ such that $\sigma_1(P_1, P_2) = \sigma_1(P_1) \cap \sigma_1(P_2) \neq \emptyset$, then, using the Taylor expansion on this intersection for these polynomials and their derivatives we obtain

$$\begin{cases} |P_j(w)|_p \ll 2^{-t}, \\ |P_j'(w)|_p \ll 2^{-2t/3}, \ j = 1, 2. \end{cases} \tag{66}$$

The polynomial $R(w) = P_1(w) - P_2(w)$ is linear. Thus we can write $R(w) = aw + b$. Then the system of inequalities (66) for R will be

$$\begin{cases} |aw + b|_p \ll 2^{-t}, \\ |a|_p \ll 2^{\frac{2t}{3}}, \\ \max(|a|, |b|) \leqslant 2Q. \end{cases} \tag{67}$$

The system of inequalities (67) is analogous to the system (42). We estimate the measure of the set of $w \in \mathbb{Q}_p$, such that the system (67) has solutions in polynomials in the same way as we did when analyzing (42). We obtain that the measure is $\ll 2^{-t/3}$. Again, $\sum_{t>t_0} 2^{-t/3} < \frac{\mu(K)}{32}$.

Summing all the estimates for cases 1–4 together we finally obtain that $\mu(M_n''(v)) < \frac{\mu(K)}{4}$ as required.

References

[1] *V. Beresnevich*, On approximation of real numbers by real algebraic numbers // Acta Arith. **90**, 1999, no. 2, P. 97 – 12.

[2] *V. Beresnevich, V. Bernik, E. Kovalevskaya*, On approximation of p–adic numbers by p–adic algebraic numbers. J. Number Theory, **111**, 2005, no. 1, P. 33 – 56.

[3] *V. Bernik*, On the exact order of approximation of zero by values of integral polynomials // Acta Arith. **53**, 1989, P. 17 – 28.

[4] *V. Bernik, H. Dickinson, J. Yuan*, Inhomogeneous Diophantine approximation on polynomials in $\mathbb{Q}_p$. Acta Arith. **90**, 1999, no. 1, P. 37 – 48.

[5] *V. Bernik, M. Dodson*, Metric Diophantine approximation on manifolds. Cambridge Tracts in Mathematics, 137. Cambridge University Press, Cambridge, 1999.

[6] *J. Cassels*, Local Fields, Cambridge University Press, Cambridge, 1986.

[7] *K. Győry*, Polynomials and binary forms with given discriminant // Publ. Math. Debrecen, **69/4**, 2006, P. 473 – 499.

[8] *E. Lutz*, Sur les approximations diophantiennes lineaires et p–adiques, Hermann, Paris, 1955.

[9] *K. Mahler*, Uber das Mass der Menge aller S–Zahlen, Math. Ann., **106**, 1932, P. 131 – 139.

[10] *W. Schmidt*, Diophantine Approximation. Lecture Notes in Mathematics, Berlin, Heidelberg, Springer-Verlag, 1980.

[11] *V.G. Sprindzuk*, Mahler's problem in metric Number Theory // Nauka i Tehnika, Minsk 1967 [Transl. Math. Monogr. **25**, Amer. Math. Soc., Providenca, R.I., 1969].

[12] *B.L. Van Der Warden*, Algebra, Berlin, Heidelberg, Springer-Verlag, 1971.

Institute of Mathematics
Surganova str. 11
220072, Minsk,
Belarus
E-mail: bernik@im.bas-net.by
olga_kukso@tut.by

Universität Bielefeld
Fakultät für Mathematik
Postfach 10 01 31
33501 Bielefeld
Germany
E-mail: goetze@math.uni-bielefeld.de

Received