

***P*-ADIC ROOT SEPARATION FOR QUADRATIC AND CUBIC POLYNOMIALS**

TOMISLAV PEJKOVIĆ

ABSTRACT. We study p -adic root separation for quadratic and cubic polynomials with integer coefficients. The quadratic and reducible cubic polynomials are completely understood, while in the irreducible cubic case and $p \neq 2$, we give a family of polynomials with the bound which is the best currently known.

1. INTRODUCTION

For a polynomial with integer coefficients, we can look at how close two of its roots can be. This can be done when we look at roots in the field of real or complex numbers and also if we wish to study roots in the p -adic setting. Since we can always find polynomials with roots as close as desired, we need to introduce some measure of size for polynomials with which we can compare this minimal separation of roots. This is done by bounding the degree and most usually using the height, i.e. maximum of the absolute values of the coefficients of a polynomial. The height of an integer polynomial $P(X)$ is denoted by $H(P)$.

For an integer polynomial $P(X)$ of degree $d \geq 2$, height $H(P)$ and with distinct roots $\alpha_1, \dots, \alpha_d \in \mathbb{C}$, we set

$$\text{sep}(P) = \min_{1 \leq i < j \leq d} |\alpha_i - \alpha_j|$$

and define $e(P)$ by

$$\text{sep}(P) = H(P)^{-e(P)}.$$

2010 *Mathematics Subject Classification.* 11C08, 11B37, 11J61.

Key words and phrases. integer polynomials, root separation, p -adic numbers.

For an infinite set S of integer polynomials containing polynomials of arbitrary large height, we define

$$e(S) = \limsup_{P(X) \in S, H(P) \rightarrow +\infty} e(P).$$

Mahler [11] proved in 1964 that if S contains only polynomials of degree d , then $e(S) \leq d - 1$. The lower bound on $e(S)$ for this class of polynomials has been successively improved. The best bound in the real/complex case is now standing at $e(S) \geq \frac{2d-1}{3}$ for general d (see [4]). However, for the set of cubic polynomials it was shown [7, 15] that $e(S) \geq 2$ which is, of course, best possible. For other small d , better results than the general one we mentioned have been found (see [6]). Another direction of research is to study particular subsets of all polynomials of degree d , for example, we can distinguish between irreducible and reducible polynomials or monic and nonmonic polynomials (see [3, 4, 5] for details).

Separation of roots in the p -adic setting has been much less studied (see [2, §9.3] and [13]). We fix our notation with respect to the p -adic analysis we will be using. Let p be a rational prime number. We denote by \mathbb{Q}_p the completion of the field of rational numbers \mathbb{Q} with respect to p -adic absolute value $|\cdot|_p$ which is normalised in such a way that $|p|_p = p^{-1}$. Also, $v_p(x) = -\log(|x|_p)/\log p$ is the usual p -adic valuation. By \mathbb{Z}_p we denote the ring of p -adic integers. We use \mathbb{C}_p for the (metric) completion of an algebraic closure of \mathbb{Q}_p . The field \mathbb{Q}_p of p -adic numbers is usually considered as an analogue of the field \mathbb{R} of real numbers, while the field \mathbb{C}_p is analogous to the field \mathbb{C} of complex numbers. Basic facts about p -adic theory will be tacitly used, interested reader can consult e.g. [8, 9].

Just as in the real and complex setting, for a polynomial $P(X) \in \mathbb{Z}[X]$ of degree $d \geq 2$ and with distinct p -adic roots $\alpha_1, \dots, \alpha_d \in \mathbb{C}_p$, we set

$$\text{sep}_p(P) = \min_{1 \leq i < j \leq d} |\alpha_i - \alpha_j|_p$$

and we call this quantity *minimal p -adic separation of roots* of $P(X)$. The definition of $e_p(P)$ and $e_p(S)$ is now completely analogous to what was done above in the real case.

Following the lines of Mahler's proof, it can be shown (see [14, Lemma 2.3]) that the next inequality holds for a separable, integer polynomial $P(X)$ of degree $d \geq 2$:

$$(1.1) \quad \text{sep}_p(P) \geq d^{-\frac{3}{2}d} H(P)^{-d+1}.$$

In this paper we show that best possible lower bounds on $e_p(S)$ can be obtained for quadratic and reducible cubic polynomials, while in the irreducible cubic case and $p \neq 2$, we give a family with the bound $e_p(S) \geq 25/14$ which is the best currently known.

Symbols \gg and \ll used in this paper are the Vinogradov symbols. For example $A \ll B$ means $A \leq cB$ where c is some constant. We will usually say what this constant depends upon in a particular case. When $A \ll B$ and $A \gg B$, we write $A \asymp B$.

2. QUADRATIC POLYNOMIALS

Inequality (1.1) says that for a quadratic separable polynomial $P(X)$ with integer coefficients, we have $\text{sep}_p(P) \geq \frac{1}{8} H(P)^{-1}$. To show that the exponent -1 over $H(P)$ really can be attained, we can take the family of reducible polynomials

$$P_k(X) = X(X + p^k) = X^2 + p^k X, \quad k \geq 1$$

which gives $\text{sep}_p(P_k) = p^{-k} = H(P)^{-1}$. We can also look at the family of irreducible polynomials

$$P_k(X) = (-p^{2k} + p^k + 1)X^2 + (p^{2k} + 2p^k)X + p^{2k}, \quad k \geq 1$$

for which

$$\begin{aligned} \text{sep}_p(P_k) &= \left| \frac{\sqrt{(p^{2k} + 2p^k)^2 - 4(-p^{2k} + p^k + 1)p^{2k}}}{-p^{2k} + p^k + 1} \right|_p \\ &= \left| \frac{\sqrt{5p^{4k}}}{-p^{2k} + p^k + 1} \right|_p = p^{-2k} \end{aligned}$$

if $p \neq 5$. Thus, here we have $\text{sep}_p(P_k) \asymp H(P_k)^{-1}$, where the implied constants are absolute. The last asymptotic relation obviously holds even if $p = 5$.

An example with a family of monic irreducible quadratic polynomials is given in the next proposition.

PROPOSITION 2.1. *There exists a family of irreducible integer polynomials*

$$P_m(X) = X^2 + a_m X + b_m, \quad m \geq 1$$

with roots in \mathbb{Q}_p such that $a_m > b_m > 0$, $a_m \asymp p^m$ and

$$\text{sep}_p(P_m) \asymp H(P_m)^{-1},$$

where the implicit constants depend only on p .

PROOF. We first examine the case $p \neq 2$. Let g be the smallest prime such that $g \equiv 1 \pmod{4p}$. Its existence is guaranteed by Dirichlet's theorem on primes in arithmetic progressions.

Let

$$l_m = \left\lfloor \frac{p^m \sqrt{g}}{2} + \frac{1}{2} \right\rfloor.$$

Then it is easy to see that

$$(2l_m - 1)^2 < p^{2m} g < (2l_m + 1)^2$$

and we put $a_m = 2l_m + 1$. Since $(2l_m + 1)^2 - (2l_m - 1)^2 = 8l_m$, if we now set $b_m = \frac{1}{4}(a_m^2 - p^{2m}g)$, it must be $0 < b_m \leq \frac{1}{4}8l_m = 2l_m < a_m$, while $b_m \in \mathbb{Z}$ is assured by $a_m^2 \equiv (2l_m + 1)^2 \equiv 1 \pmod{4}$ and $p^{2m}g \equiv (\pm 1)^{2m}1 \equiv 1 \pmod{4}$.

Hensel's Lemma ensures that the polynomial $Q(X) = X^2 - g$ has roots $\delta \in 1 + p\mathbb{Z}_p$ and $-\delta \in -1 + p\mathbb{Z}_p$. Note that $\delta \notin \mathbb{Q}$. Thus the polynomial

$$P_m(X) = X^2 + a_m X + b_m = \frac{1}{4}((2X + a_m)^2 - p^{2m}g) = \frac{p^{2m}}{4}Q\left(\frac{2X + a_m}{p^m}\right)$$

has roots $\frac{-a_m \pm p^m \delta}{2}$, which are in $\mathbb{Q}_p \setminus \mathbb{Q}$ and their distance is

$$\text{sep}_p(P_m) = |p^m \delta|_p = p^{-m} \asymp a_m^{-1} = \mathbb{H}(P_m)^{-1}.$$

If $p = 2$, we take $l_m = \lfloor 2^m \sqrt{17} \rfloor$, and put $a_m = 2l_m + 2$. Taking $b_m = \frac{a_m^2}{4} - 2^{2m} \cdot 17$, it can easily be checked that all the claims of this proposition are fulfilled. In this case we need to use Hensel's Lemma in its more general form (see [10, Proposition 7.6, §XII.7, p. 493]). \square

Although the following proposition is quite easy, best possible constant appearing on the right-hand side of the inequality as well as conditions for equality seem to be new.

PROPOSITION 2.2. *Let $P(X)$ be a quadratic separable polynomial with integer coefficients. For every prime p , we have*

$$\text{sep}_p(P) \geq \frac{1}{\mathbb{H}(P)\sqrt{5}}.$$

Equality is achieved if and only if $p = 5$ and $P(X) \in \{X^2 \pm X - 1, -X^2 \pm X + 1\}$.

PROOF. For a separable quadratic polynomial $P(X) = aX^2 + bX + c$ with integer coefficients, the following sequence of inequalities holds

$$\begin{aligned} \text{sep}_p(P) &= \left| \frac{\sqrt{b^2 - 4ac}}{a} \right|_p \\ &= \frac{|b^2 - 4ac|_p^{\frac{1}{2}}}{|a|_p} \stackrel{(i)}{\geq} \frac{1}{|b^2 - 4ac|_p^{\frac{1}{2}}} \stackrel{(ii)}{\geq} \frac{1}{(|b|^2 + 4|a||c|)^{\frac{1}{2}}} \stackrel{(iii)}{\geq} \frac{1}{\mathbb{H}(P)\sqrt{5}}. \end{aligned}$$

In (2.2.i) equality holds if and only if p does not divide a and $b^2 - 4ac = p^k$ for some nonnegative integer k . In (2.2.ii) equality is achieved if and only if $ac \leq 0$ while equality in (2.2.iii) is equivalent to $|a| = |b| = |c| = \mathbb{H}(P)$. Combining these conditions we arrive at the statement of the proposition. \square

3. REDUCIBLE CUBIC CASE

In order to find p -adic root separation for some cubic polynomials, we will be using properties of Newton polygons. For all terminology consult [8, 9]. We copy this lemma from [8, Theorem 6.4.7] for the benefit of our reader.

LEMMA 3.1. *Let $P(X) = 1 + a_1X + a_2X^2 + \dots + a_nX^n \in \mathbb{C}_p[X]$ be a polynomial, and let m_1, m_2, \dots, m_r be the slopes of its Newton polygon in increasing order. Let i_1, i_2, \dots, i_r be the corresponding lengths. Then, for each k , $1 \leq k \leq r$, $P(X)$ has exactly i_k roots in \mathbb{C}_p (counting multiplicities) of p -adic absolute value p^{m_k} .*

We will exhibit a family of reducible cubic polynomials whose separation of roots is (up to an absolute constant) best possible.

We look at the polynomial $P(X) = (aX - b)(X^2 + rX + s) \in \mathbb{Z}[X]$. The roots of this polynomial are

$$\frac{b}{a} \quad \text{and} \quad \frac{-r \pm \sqrt{r^2 - 4s}}{2},$$

so in order to get the smallest separation of roots we only have to look at the distance of the root of the linear and of the quadratic factor of $P(X)$. Let

$$0 = P\left(\frac{b}{a} + \varepsilon\right) = \varepsilon\left(\varepsilon^2 + \left(\frac{2b}{a} + r\right)\varepsilon + \left(\frac{b^2}{a^2} + \frac{rb}{a} + s\right)\right).$$

Therefore, $\varepsilon \neq 0$ is a root of the polynomial

$$(3.3) \quad Q(X) = 1 + \frac{2ba + ra^2}{b^2 + rba + sa^2}X + \frac{a^2}{b^2 + rba + sa^2}X^2.$$

It is obvious that

$$\left| \frac{2ba + ra^2}{b^2 + rba + sa^2} \right|_p \leq |b^2 + rba + sa^2| \ll H(P)^2,$$

where the implied constant in second inequality is absolute and follows from Gelfond's Lemma (see e.g. [2, Lemma A.3, p. 221] or [1, Lemma 1.6.11, p. 27]). The same bound holds for the leading coefficient of $Q(X)$ as well. We will construct a sequence of polynomials $(P_k(X))_k$ such that the above bound becomes asymptotic equality. Then, using the Newton polygons it will follow that asymptotically $\text{sep}(P_k) \asymp H(P_k)^{-2}$ which is, of course, the best possible exponent.

To this end we will use the sequence $(A_k(n))_{k \geq 0}$ of polynomials in n defined recursively

$$A_0(n) = 1, \quad A_1(n) = 1, \quad A_{k+1}(n) = A_k(n) - n^2 A_{k-1}(n) \text{ for } n \geq 2.$$

First few terms of the sequence $A_k(n)$ are

$$1, 1, -n^2 + 1, -2n^2 + 1, n^4 - 3n^2 + 1, 3n^4 - 4n^2 + 1, \dots$$

so we see that the constant term is always 1 and the degree is $\deg_n A_k = 2\lfloor \frac{k}{2} \rfloor$.

We also have

$$\begin{aligned}
(3.4) \quad A_{k+1}^2 - A_{k+1}A_k + n^2 A_k^2 &= A_k^2 - 2n^2 A_k A_{k-1} + n^4 A_{k-1}^2 - (A_k - n^2 A_{k-1})A_k + n^2 A_k^2 \\
&= n^2 (A_k^2 - A_k A_{k-1} + n^2 A_{k-1}^2) \\
&= \dots = (n^2)^k (A_1^2 - A_1 A_0 + n^2 A_0^2) \\
&= (n^2)^{k+1} = n^{2(k+1)}.
\end{aligned}$$

Fixing any integer $k \geq 2$, we set

$$a_{k,l} = A_k(p^l), \quad b_{k,l} = A_{k+1}(p^l), \quad r_{k,l} = -1, \quad s_{k,l} = p^{2l}, \quad \text{for } l \geq 1.$$

Denoting

$$\begin{aligned}
P_{k,l}(X) &= (a_{k,l}X - b_{k,l})(X^2 + r_{k,l}X + s_{k,l}) \\
&= (A_k(p^l)X - A_{k+1}(p^l))(X^2 - X + p^{2l}), \quad l \geq 1,
\end{aligned}$$

we see that the quadratic factor is irreducible over \mathbb{Q} and (dropping indices k and l)

$$v_p\left(\frac{2ba + ra^2}{b^2 + rba + sa^2}\right) = -2(k+1)l$$

since $a \equiv b \equiv 1 \pmod{p}$ and $b^2 + rba + sa^2 = p^{2(k+1)l}$ because of (3.4). Therefore, Lemma on Newton polygons and (3.3) imply that

$$\text{sep}_p(P_{k,l}) = |\varepsilon|_p = p^{-2(k+1)l}.$$

Since $|a| \asymp_k p^{2\lfloor k/2 \rfloor l}$ and $|b| \asymp_k p^{2\lfloor (k+1)/2 \rfloor l}$, we have

$$\mathbb{H}(P_{k,l}) \asymp_k p^{2(\lfloor (k+1)/2 \rfloor + 1)l},$$

and thus

$$p^{(k+2)l} \ll_k \mathbb{H}(P_{k,l}) \ll_k p^{(k+3)l},$$

where we alluded by \asymp_k and \ll_k that the implied constants depend on k as well as on p which is not mentioned so as not to encumber notation needlessly. This leads to

$$\text{sep}_p(P_{k,l}) = \mathbb{H}(P_{k,l})^{-2+\varepsilon_{k,l}}, \quad l \rightarrow \infty.$$

Here, we have $\varepsilon_{k,l} \in [\frac{1}{k+2}, \frac{5}{k+3}]$ when l is large enough with respect to k . Obviously, $\varepsilon_{k,l} \rightarrow 0$ when $k \rightarrow \infty$. Hence, we can choose $P_k(X) = P_{k,l_k}(X)$ for some sequence $(l_k)_k$ which increases sufficiently fast so that

$$\text{sep}_p(P_k) = \mathbb{H}(P_k)^{-2+\varepsilon_k},$$

while $\mathbb{H}(P_k) \rightarrow \infty$ and $\varepsilon_k \rightarrow 0$ when $k \rightarrow \infty$.

4. IRREDUCIBLE CUBIC CASE

Let $P(X) = aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$ be an integer polynomial with distinct roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}_p$. In order to analyze $\text{sep}_p(P)$, we first construct a polynomial whose roots are closely related to the distances between the roots of $P(X)$. Denote by $Q(X) = \text{Res}_Y(P(Y), P(X+Y))$, the resultant of polynomials $P(Y)$ and $P(X+Y)$ with respect to variable Y . Standard properties of resultants (consult for example [10, 12]) tell us that $Q(X)$ has integer coefficients and for $x_0 \in \mathbb{C}_p$, we have

$$\begin{aligned} Q(x_0) = 0 &\Leftrightarrow P(Y) \text{ and } P(x_0 + Y) \text{ have a common root in } \mathbb{C}_p \\ &\Leftrightarrow \exists y_0 \in \mathbb{C}_p \text{ such that } P(y_0) = P(x_0 + y_0) = 0 \\ &\Leftrightarrow \exists \alpha, \beta \in \mathbb{C}_p \text{ such that } P(\alpha) = P(\beta) = 0, x_0 = \alpha - \beta \end{aligned}$$

This shows that if we denote $\delta_1 = \alpha_1 - \alpha_2$, $\delta_2 = \alpha_2 - \alpha_3$, $\delta_3 = \alpha_3 - \alpha_1$, then

$$Q(X) = \tilde{a} \prod_{\substack{1 \leq i < j \leq 3}} (X - (\alpha_i - \alpha_j)) = \tilde{a}(X^2 - \delta_1^2)(X^2 - \delta_2^2)(X^2 - \delta_3^2)X^3.$$

Taking $R(X) = Q(X)/X^3 \in \mathbb{Z}[X]$ and then $S(X) = R(\sqrt{X})/R(0)$, we get that

$$S(X) = \frac{-1}{\delta_1^2 \delta_2^2 \delta_3^2} (X - \delta_1^2)(X - \delta_2^2)(X - \delta_3^2)$$

is a polynomial in $\mathbb{Q}[X]$ such that

$$(4.5) \quad S(0) = 1 \quad \text{and} \quad \text{sep}_p(P) = \min \{ |\delta|_p^{\frac{1}{2}} : \delta \in \mathbb{C}_p, S(\delta) = 0 \}.$$

After some computation, we obtain

$$(4.6) \quad S(X) = 1 - \frac{(b^2 - 3ac)^2 X}{b^2 c^2 - 4ac^3 - 4b^3 d + 18abcd - 27a^2 d^2} + \frac{2a^2 (b^2 - 3ac) X^2}{b^2 c^2 - 4ac^3 - 4b^3 d + 18abcd - 27a^2 d^2} - \frac{a^4 X^3}{b^2 c^2 - 4ac^3 - 4b^3 d + 18abcd - 27a^2 d^2}.$$

Note that $b^2 c^2 - 4ac^3 - 4b^3 d + 18abcd - 27a^2 d^2$ is exactly the discriminant of polynomial $P(X)$.

Let us describe the process by which we arrive at the family of polynomials with the best currently known bound for separation of roots. We search for cubic polynomials in X with coefficients that are polynomials in n . We want the discriminant with respect to X to be a polynomial of small degree in n . The polynomial

$$(-44n^3 - 60n^2 - 3n)X^3 + (36n^3 + 24n^2 - 21n)X^2 + (36n^2 + 39n)X + 9n + 8$$

has discriminant $\asymp n^3$. Substituting $n \mapsto n^3$ and $X \mapsto X/n$, we obtain the polynomial

$$(-44n^6 - 60n^3 - 3)X^3 + (36n^7 + 24n^4 - 21n)X^2 + (36n^5 + 39n^2)X + 9n^3 + 8$$

with discriminant $\asymp n^3$. Since the discriminant is quite small compared to the height of the given polynomial, we expect that the roots in \mathbb{C} are quite close. In order to get the polynomial with small discriminant in the p -adic value, we proceed with the following “reversion”. Substituting $n \mapsto 1/n$ in the previous polynomial and then multiplying by n^7 gives

$$(-3n^7 - 60n^4 - 44n)X^3 + (-21n^6 + 24n^3 + 36)X^2 + (39n^5 + 36n^2)X + 8n^7 + 9n^4,$$

which has the discriminant $-1728(4n^{25} + 9n^{28})$ and now putting $n = p^k$, we would get a polynomial with very small p -adic absolute value of the discriminant. Unfortunately, we have no way of knowing that this polynomial is irreducible. In order not to repeat previous construction from the start, we simply do the following to the last polynomial

$$n \mapsto 2^{-5/3}3^{2/3}p^k, \quad X \mapsto 2^{2/3}3^{4/3}X, \quad \text{multiply with } 2^{29/3}3^{-14/3}$$

and obtain the family of polynomials

$$P_k(X) = (-45056p^k - 17280p^{4k} - 243p^{7k})X^3 + (8192 + 1536p^{3k} - 378p^{6k})X^2 \\ + (512p^{2k} + 156p^{5k})X + 8p^{4k} + 2p^{7k}.$$

Now the coefficients of $S(X) = a_0 + a_1X + a_2X^2 + a_3X^3$ in the order a_0, a_1, a_2, a_3 are

$$1, \frac{256p^{-25k} (2097152 + 9p^{3k} (327680 + 99p^{3k} (1536 + 256p^{3k} + 9p^{6k})))^2}{19683 (128 + 81p^{3k})}, \\ - \frac{16p^{-23k} (45056 + 27p^{3k} (640 + 9p^{3k}))^2}{19683 (128 + 81p^{3k})}, \\ \cdot (2097152 + 9p^{3k} (327680 + 99p^{3k} (1536 + 256p^{3k} + 9p^{6k}))), \\ \frac{p^{-21k} (45056 + 27p^{3k} (640 + 9p^{3k}))^4}{78732 (128 + 81p^{3k})},$$

which gives the following points we are interested in (for $p \neq 2$)

$$(0, v_p(a_0)), (1, v_p(a_1)), (2, v_p(a_2)), (3, v_p(a_3)) \\ = (0, 0), (1, -25k), (2, -23k), (3, -21k).$$

Looking at the Newton polygon obtained from these points and using (4.5), we see that $\text{sep}_p(P_k) = p^{-25k/2} \asymp H(P_k)^{-25/14}$ because $H(P_k) \asymp p^{7k}$. Even if asymptotics does not change for $p = 2$, we are not certain that the polynomials $P_k(X)$ are irreducible in this case. For $p \neq 2$ this is guaranteed by Eisenstein’s criterion.

REMARK 4.1. This last family of polynomials was deduced from the family

$$(-45056n^6 - 17280n^3 - 243)X^3 + (8192n^7 + 1536n^4 - 378n)X^2 \\ + (512n^5 + 156n^2)X + 8n^3 + 2, \quad n \geq 0$$

by the usual process of “reversion”. The original family of polynomials gives a separation of roots in the real case with the exponent $-25/14$ which is at present the best exponent for a family of irreducible cubic polynomials with polynomial growth of coefficients. Although Schönhage [15] proved that in the real case the best possible exponent -2 is attainable, his families of polynomials have exponential growth of coefficients. One of the main ingredients Schönhage used to construct these families is continued fraction expansion of real numbers. In the p -adic setting there are several types of continued fractions that have been proposed. None of them have all the good properties of the standard continued fractions and at the moment Schönhage’s construction does not seem to translate easily to p -adic numbers. This is one of the reasons why we are interested in families of polynomials with polynomial growth of coefficients.

ACKNOWLEDGEMENTS.

The author was supported by the Croatian Science Foundation under the project no. 6422.

REFERENCES

- [1] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006.
- [2] Y. Bugeaud, *Approximation by algebraic numbers*, Cambridge Tracts in Mathematics, Cambridge, 2004.
- [3] Y. Bugeaud and A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc. **43** (2011), 1239–1244.
- [4] Y. Bugeaud and A. Dujella, *Root separation for reducible integer polynomials*, Acta Arith. **162** (2014), 393–403.
- [5] Y. Bugeaud and M. Mignotte, *Polynomial root separation*, Intern. J. Number Theory **6** (2010), 587–602.
- [6] A. Dujella and T. Pejković, *Root separation for reducible monic quartics*, Rend. Semin. Mat. Univ. Padova **126** (2011), 63–72.
- [7] J.-H. Evertse, *Distances between the conjugates of an algebraic number*, Publ. Math. Debrecen **65** (2004), 323–340.
- [8] F. Q. Gouvêa, *p -adic numbers. An introduction*, Second edition, Universitext, Springer-Verlag, Berlin, 1997.
- [9] N. Koblitz, *p -adic numbers, p -adic analysis, and zeta-functions*, Second edition, Graduate Texts in Mathematics, 58. Springer-Verlag, New York, 1984.
- [10] S. Lang, *Algebra*, Revised third edition, Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.
- [11] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.
- [12] M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag, New York, 1992.

- [13] J. F. Morrison, *Approximation of p -adic numbers by algebraic numbers of bounded degree*, J. Number Theory **10** (1978), no. 3, 334–350.
- [14] T. Pejković, *Polynomial Root Separation and Applications*, PhD Thesis, Université de Strasbourg, Strasbourg, 2012.
- [15] A. Schönhage, *Polynomial root separation examples*, J. Symbolic Comput. **41** (2006), 1080–1090.

P -adska separacija korijena kvadratnih i kubnih polinoma

Tomislav Pejković

SAŽETAK. Promatramo p -adsku separaciju korijena za kvadratne i kubne polinome s cjelobrojnim koeficijentima. Slučajevi kvadratnih i reducibilnih kubnih polinoma potpuno su riješeni. Za ireducibilni kubni slučaj i $p \neq 2$, dana je familija polinoma s najboljom do sada poznatom separacijom.

Tomislav Pejković
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
E-mail: pejkovic@math.hr