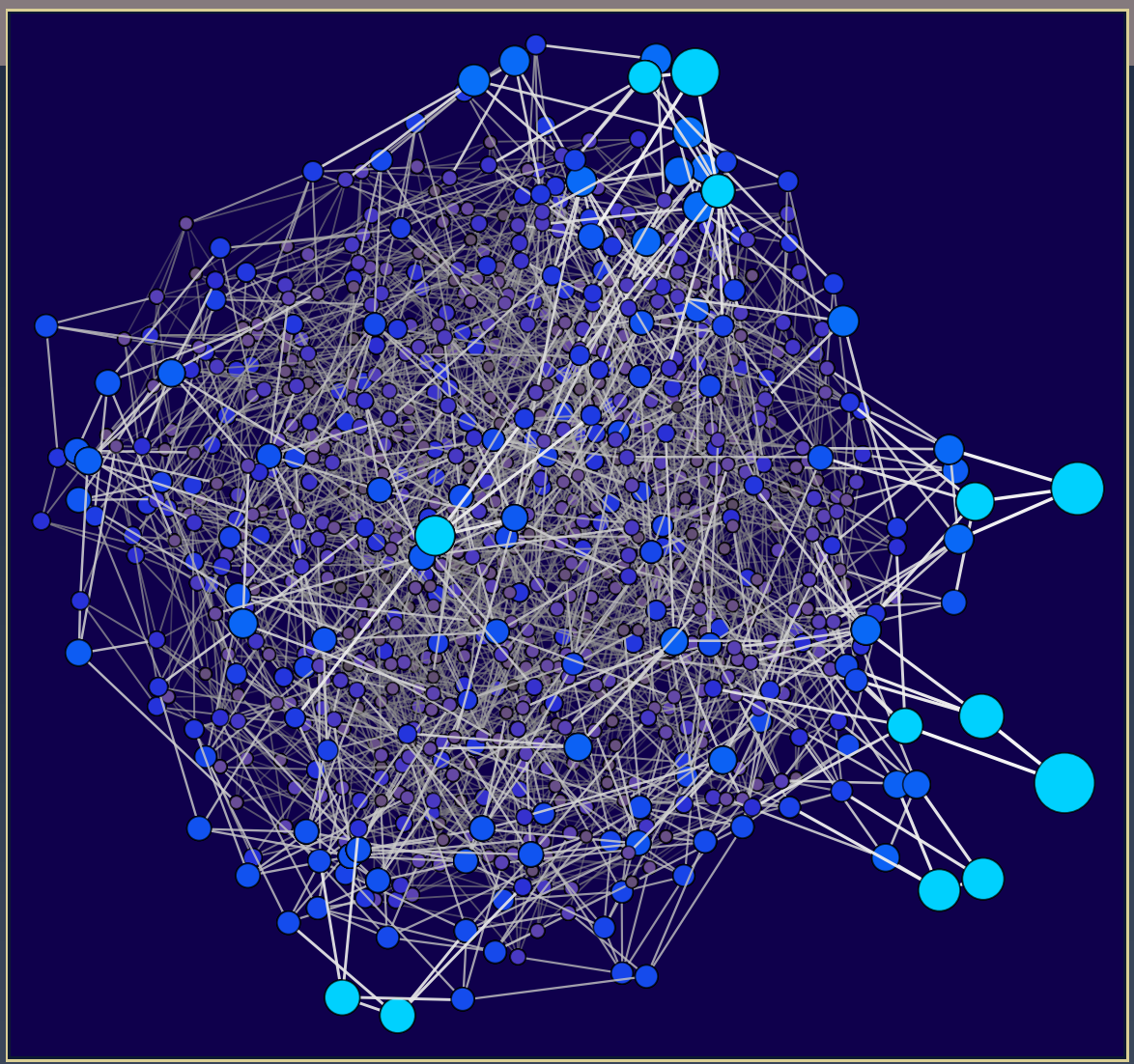
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Totally p-adic numbers of degree 3

Emerald Stacy



msp

THE OPEN BOOK SERIES **4** (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.387

msp

Totally p-adic numbers of degree 3

Emerald Stacy

The height of an algebraic number α is a measure of how arithmetically complicated α is. We say α is totally p-adic if the minimal polynomial of α splits completely over the field $\mathbb{Q}_p$ of p-adic numbers. We investigate what can be said about the smallest nonzero height of a degree 3 totally p-adic number.

1. Introduction

Recall that an algebraic number α is *totally p-adic* (respectively, totally real) if the minimal polynomial of α, $f_\alpha \in \mathbb{Q}[x]$, splits completely over $\mathbb{Q}_p$ (respectively, $\mathbb{R}$). We will denote by $h(\alpha)$ the logarithmic Weil height of α [BG06].

In 1975, Schinzel used the arithmetic-geometric mean inequality to prove that if α is a totally real algebraic integer, with $\alpha \neq 0, \pm 1$, then

$$h(\alpha) \geq \tfrac{1}{2} \log\left(\tfrac{1+\sqrt{5}}{2}\right)$$

with equality if $\alpha = \frac{1}{2}(1+\sqrt{5})$ [Sch75]. In 1993, Höhn & Skoruppa used an auxiliary function to provide an alternate proof of Schinzel's bound [HS93]. Bombieri & Zannier [BZ01] proved that an analogue to Schinzel's theorem holds in $\mathbb{Q}_p$ for each prime p, although the analogous best possible lower bound is unknown.

Additionally, there have been some results constructing totally p-adic (or totally real) algebraic numbers of small height. In particular, these results provide an upper bound on the smallest height attained by α under certain splitting conditions. The degree of a totally p-adic number is the degree of its minimal polynomial with coefficients in $\mathbb{Z}$. Petsche [Pet] proved that for odd primes p, there exists some totally p-adic $\alpha \in \overline{\mathbb{Q}}$ of degree $d \leq p-1$, and

$$0 < h(\alpha) \leq \tfrac{1}{p-1} \log\left(\frac{p+\sqrt{p^2+4}}{2}\right).$$

MSC2010: 11G50, 11S20, 11Y40, 12Y05.
Keywords: height, algorithm, p-adic.

Recently, Pottmeyer [Pot18] has improved upon Petsche's upper bound, and obtained the existence of totally p-adic α such that

$$0 < h(\alpha) \leq \frac{\log p}{p}.$$

In 1980, Smyth created a set of totally real numbers of small height by taking all preimages of 1 under the map $\phi(x) = x - \frac{1}{x}$. The heights of the points in this set have a limit point $\ell \approx 0.27328$ [Smy80]. In [PS19], Petsche and Stacy use an argument inspired by this result of Smyth to provide an upper bound on the smallest limit point of heights of totally p-adic numbers of degree d.

In this paper, we fix the degree d to be 3 and let the prime p vary. In particular, we define $\tau_{d,p}$ to be the smallest height attained by a totally p-adic, nonzero, nonroot of unity, algebraic number of degree d. For any pair d and p, we know $\tau_{d,p} < \infty$ since we can construct a Newton polygon for an irreducible polynomial of degree d that splits completely over $\mathbb{Q}_p$ [Cas86].

In this paper, we develop tools to determine $\tau_{3,p}$ for all $p \geq 5$. In Section 2, we develop and prove an algorithm to determine $\tau_{3,p}$ for a given prime p, which we implement in Section 2.5. All code was written for SageMath, version 8.2, and is included within Section 2.5. A table of results can be found in Section 3, and Section 4 describes future areas of interest.

2. The algorithm

In Section 2.1, we prove that $\tau_{3,p} \leq 0.70376$ for all $p \geq 5$. To do so, we establish that for every prime p, there is a cubic polynomial with an abelian Galois group that splits completely over $\mathbb{Q}_p$. By the height-length bound [BG06, Proposition 1.6.7], a list of all cubic polynomials with length less than 68 will contain all irreducible, noncyclotomic, cubic polynomials with roots of height less than 0.70376. By the Northcott property there are only finitely many such polynomials, and thus we have a finite list to check for $\tau_{3,p}$ and our algorithm will terminate.

In Section 2.2, we use the method of Cardano to determine the roots of a cubic polynomial. In Sections 2.3 and 2.4, we establish criteria to determine if those roots are in $\mathbb{Q}_p$. The criteria are different depending if $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$, since $\mathbb{Q}_p$ contains a primitive cube root of unity if and only if $p \equiv 1 \pmod 3$. In Section 2.5, we implement the algorithm, the results of which can be found in Section 3.

2.1. ***Establishing termination.*** To establish that our algorithm will terminate, we create a finite list of polynomials, and verify that for each prime, there must be a polynomial in our list that will split completely over $\mathbb{Q}_p$.

Let f_α denote the minimal polynomial of α. Then $h(\alpha) = \frac{1}{3} \log M(f_\alpha)$, where $M(f_\alpha)$ is the Mahler measure of f_α. Thus, if $M(f_\alpha) \leq 8.5$, then $h(\alpha) \leq 0.71335$. The function `mahler_measure_cubic` calculates the Mahler measure of the cubic polynomial

$$f(x) = ax^3 + bx^2 + cx + d :$$

```
def mahler_measure_cubic(a,b,c,d):
    M = a
    Poly = a*x^3 + b*x^2 + c*x + d
    Roots = Poly.roots(CC)
    for i in [0..len(Roots)-1]:
        M = M * max(1,abs(Roots[i][0]))
    return M.n(digits=10)
```

For $f(x) = \sum_{i=0}^{d} a_i x^i$, the *length* of f is $L(f) = \sum_{i=0}^{d} |a_i|$. The length will be useful to us since for any polynomial f,

$$L(f) \leq 2^d M(f),$$

where $d = \deg f$ [BG06, Proposition 1.6.7]. Thus, the following program generates a list of all cubic polynomials with

$$L(f) \leq 2^3(8.5) = 68$$

and removes any polynomial that is either reducible or has Mahler measure greater than 8.5. We use the built-in Sage function `is_irreducible()` to determine if a polynomial is irreducible over $\mathbb{Q}$.

In addition to the polynomial and Mahler measure, the list also stores the coefficients of the cubic in its so-called depressed form ($x^3 + Ax + B$), the discriminant of the polynomial, and the height of the roots. For more information on depressing a cubic, please see Section 2.2.

The command `sorted()` will reorganize the array in ascending order of the first value — in this case it will sort by Mahler measure, which is equivalent to sorting by height. The output of this program is 26796 polynomials that are saved as the file `irred_polynomials_L68`. Runtime was 124 minutes.

```
R.<x> = QQ[]
Polynomials=[]
L=68
for a in [1..L]:
    for b in [-L+abs(a)..L-abs(a)]:
        for c in [-L+abs(a)+abs(b)..L-abs(a)-abs(b)]:
            for d in [-L+abs(a)+abs(b)+abs(c)..L-abs(a)-abs(b)-abs(c)]:
                Poly = a*x^3 + b*x^2 + c*x + d
                if Poly.is_irreducible()==True:
                    MM = mahler_measure_cubic(a,b,c,d)
                    A = (3*a*c - b^2 ) / (3*a^2 )
                    B = (27*a^2*d - 9*a*b*c + 2*b^3 ) / (27*a^3 )
                    Delta = B^2 + 4 * A^3 / 27
                    h = 1/3 * log(MM);
                    if MM <= L/8:
                        Polynomials.append([MM,a,b,c,d,A,B,Delta,h])
Polynomials=sorted(Polynomials)
```

Next, we remove from this list all polynomials with nonabelian Galois group. In general, the Galois group of a polynomial $f(x) \in \mathbb{Z}[x]$ of degree d is isomorphic to a subgroup of A_d if and only if the discriminant of f is a square in $\mathbb{Q}$ [Con18, Theorem 1.3]. In the case of f cubic, the Galois group of f is A_3, and thus abelian, if and only if the discriminant of f is a square in $\mathbb{Q}$.

Let K be the number field created by adjoining the roots of f to $\mathbb{Q}$ and let Δ be the discriminant of K. By the Kronecker–Weber theorem, K must be contained within a cyclotomic extension of $\mathbb{Q}$. Let m be the

conductor of K, meaning the smallest m such that K is a subfield of $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m-th root of unity. To calculate the conductor, we turn to a special case of the Hasse conductor-discriminant formula, as follows.

Theorem 1 [Has30, Theorem 6]. *Let K be an abelian extension of $\mathbb{Q}$, with $[K : \mathbb{Q}] = 3$ and discriminant Δ. Let $p_1, p_2, \ldots, p_n$ be all the primes (aside from 3) that divide Δ. If 3 divides Δ, then the conductor of K is $9p_1p_2\cdots p_n$. If 3 not does divide Δ, then the conductor of K is $p_1p_2\cdots p_n$.*

The following program begins by identifying if each cubic polynomial has an abelian Galois group. If so, then the program calculates the discriminant of K (the number field obtained by adjoining the roots of f to $\mathbb{Q}$) by applying the built-in function `absolute_discriminant()`. It then applies Theorem 1 and uses the built-in Sage command `factor()` to determine the conductor of K. All of this output is stored in the array `AbelianCubics`, which contains the information for 156 polynomials.

```
Polynomials=load('irred_polynomials_L68')
L=len(Polynomials)
AbelianCubics=[]
for i in [0..L-1]:
    Poly = Polynomials[i];
    a = Poly[1];
    b = Poly[2];
    c = Poly[3];
    d = Poly[4];
    D = b^2*c^2 - 4*a*c^3 - 4*b^3*d - 27*a^2*d^2 + 18*a*b*c*d;
    if D.is_square()==True:
        K.<j> = NumberField(a*x^3 + b*x^2 + c*x + d)
        DD = K.absolute_discriminant()
        MM = Poly[0];
        h = Poly[8];
        Factors = DD.factor()
        list_of_factors = list(Factors)
        L = len(list_of_factors)
        Cond = 1
        for i in [0..L-1]:
            Cond = Cond*list_of_factors[i][0]
            if list_of_factors[i][0]==3:
                Cond = Cond*3
        C = Cond
        AbelianCubics.append([h, a*x^3 + b*x^2 + c*x + d ,DD,C]);
```

The following lemma is well known, but for lack of a convenient reference, we provide a proof.

Lemma 2. *Let $\alpha \in \mathbb{Q}(\zeta_n)$ have minimal polynomial $f_\alpha \in \mathbb{Z}[x]$, and let*

$$G_\alpha = \{[i] \in (\mathbb{Z}/n\mathbb{Z})^\times \mid \sigma_i(\alpha) = \alpha\},$$

where $\sigma_i(\zeta_n) = \zeta_n^i$. Thus G_α is the subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ corresponding to $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\alpha))$ via the isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let $p \nmid n$ be a prime. Then f_α splits completely in $\mathbb{Q}_p$ if and only if $[p] \in G_\alpha$.

Proof. The automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ satisfies $\sigma_p(x) \equiv x \pmod{p}$ for all $x \in \mathbb{Z}[\zeta_n]$ [Bak06, Lemma 4.51]. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an abelian extension, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension and therefore σ_p

restricts to an automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$; the above congruence implies that σ_p is the Frobenius element of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ associated to the prime p.

If $[p] \in G_\alpha$, then σ_p is the identity element of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$, which implies that p splits completely in $\mathbb{Q}(\alpha)$ [Bak06, Proposition 4.36]; that is $p\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathfrak{p}_1 \cdots \mathfrak{p}_d$, where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. It follows that each local degree $e(\mathfrak{p}_i/p) f(\mathfrak{p}_i/p) = [\mathbb{Q}(\alpha)_{\mathfrak{p}_i} : \mathbb{Q}_p]$ is equal to 1 [Bak06, Theorem 5.25], which means that $\mathbb{Q}(\alpha)_{\mathfrak{p}_i} = \mathbb{Q}_p$ for $i = 1, 2, \ldots, d$. In particular, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}_p$, and therefore as $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, all d of the Galois conjugates of α are in $\mathbb{Q}_p$ as well. Hence $f_\alpha(x)$ splits completely in $\mathbb{Q}_p$. The converse follows from a straightforward reversal of this argument. □

For each polynomial f_α in `AbelianCubics`, we want to determine the congruence classes modulo m of a prime p for f_α to split completely in $\mathbb{Q}_p$, where m is the conductor of the splitting field of f_α. The following code goes through each line in the array `AbelianCubics`, and for each polynomial f_α in the list, computes the set $B_\alpha \subseteq (Z/mZ)^\times$ so that f_α splits completely in $\mathbb{Q}_p$ if and only if $[p] \in B_\alpha$, where $[p]$ denotes the residue of $p \pmod m$.

Note that if $(\mathbb{Z}/m\mathbb{Z})^\times$ has a unique index 3 subgroup, then this group must be G_α. In the case that $(\mathbb{Z}/m\mathbb{Z})^\times$ does not have a unique index 3 subgroup, we check the first 50 primes to determine if there is a root in $\mathbb{Q}_p$ via Hensel's lemma. When a root of f_α is determined to be in $\mathbb{Q}_p$, we know that for all primes q with $q \equiv p \pmod m$, f_α must split completely in $\mathbb{Q}_p$, by Lemma 2. Further, we know there are $|(\mathbb{Z}/m\mathbb{Z})^\times|/3$ congruence classes for which f_α splits completely in $\mathbb{Q}_p$. Thus, after testing the first 50 primes, the code checks the cardinality of the set of congruences to ensure all were found. For this particular list of polynomials, 50 is sufficient to identify the index 3 subgroup.

```
AbelianCubics=load('AbelianCubics')
L=len(AbelianCubics);
P = Primes();
for i in [0..L-1]:
    Poly = AbelianCubics[i][1]
    PolyList = Poly.list()
    a = PolyList[3]
    b = PolyList[2]
    c = PolyList[1]
    d = PolyList[0]
    Cond = AbelianCubics[i][3]
    v = [1];
    for j in [0..50]:
        for k in [1..P[j]-1]:
            M = Integer( a*k^3 + b*k^2 + c*k + d )
            M = M%P[j]
            N = Integer( 3*a*k^2 + 2*b*k + c )
            N = N%P[j]
            if M==0 and N>0:
                v.append(P[j]%Cond)
    V = sorted(v)
    V = set(V)
```

The results of this code are included as an online supplement to this paper. A sampling of the data is included in Table 1 for reference.

$h(\alpha)$	f_α	α is totally p-adic if and only if
0.26986	$x^3 - x^2 - 2x + 1$	$p \equiv 1, 6 \pmod 7$
0.35252	$x^3 - 3x^2 + 1$	$p \equiv 1, 8 \pmod 9$
0.60981	$3x^3 - 4x^2 - 5x + 3$	$p \equiv 1, 3, 8, 9, 11, 20, 23, 24, 27, 28, 33, 34, 37, 38, 41, 50, 52, 53, 58, 60 \pmod{61}$
0.69106	$3x^3 - x^2 - 8x + 3$	$p \equiv 1, 3, 7, 8, 9, 10, 17, 21, 22, 24, 27, 30, 43, 46, 49, 51, 52, 56, 63, 64, 65, 66, 70, 72 \pmod{73}$
0.69903	$2x^3 - 9x^2 + 3x + 2$	$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63}$
0.70376	$x^3 - 9x^2 + 6x + 1$	$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}$

Table 1. A sample of the data included in the online supplement.

Theorem 3. *Let p be a prime. Then $\tau_{3,p} \leq 0.70376$.*

Proof. For a prime p, denote by $\tau_{3,p}^{\text{ab}}$ the smallest nontrivial height of an abelian, cubic, totally p-adic number. Note that $\tau_{3,p} \leq \tau_{3,p}^{\text{ab}}$. Thus, if we show that $\tau_{3,p}^{\text{ab}} \leq 0.70376$, we have proven the theorem.

Based on the results from Table 1, we know

$$\tau_{3,3}^{\text{ab}} \leq 0.609817669 \quad \text{and} \quad \tau_{3,7}^{\text{ab}} \leq 0.501878627.$$

All primes $p \neq 3, 7$, when reduced modulo 63, are contained in $(\mathbb{Z}/63\mathbb{Z})^\times$. Observe that

$$(\mathbb{Z}/63\mathbb{Z})^\times = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20, 22, 23, 25, 26, 29, 31, 32, 34, 37, 38, 40, 41, 43, 44, 46, 47, 50, 52, 53, 55, 58, 59, 61, 62\}.$$

Further, we observe that

$$\tau_{3,p}^{\text{ab}} \leq \begin{cases} 0.269862305 & \text{if } p \equiv 1, 6 \pmod 7, \\ 0.352525605 & \text{if } p \equiv 1, 8 \pmod 9. \end{cases}$$

Thus

$$\tau_{3,p}^{\text{ab}} \leq 0.269862305 \text{ for } p \equiv 1, 8, 13, 20, 22, 29, 34, 41, 43, 50, 55, 62 \pmod{63},$$
$$\tau_{3,p}^{\text{ab}} \leq 0.352525605 \text{ for } p \equiv 10, 17, 19, 26, 37, 44, 46, 53 \pmod{63}.$$

It remains to determine an upper bound on $\tau_{3,p}^{\text{ab}}$ for

$$p \equiv 2, 4, 5, 11, 16, 23, 25, 31, 32, 38, 40, 47, 52, 58, 59, 61 \pmod{63}.$$

Note that each of the above numbers falls into one of the following two sets:

$$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63},$$
$$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}.$$

Further, we observe that by the last two lines of Table 1, given any prime p, one of the polynomials in the table must split completely over $\mathbb{Q}_p$. □

2.2. ***Determining roots of cubic polynomials.*** In *Ars Magna*, Cardano describes a method to find the roots of a cubic polynomial f as elements of $\mathbb{C}$ [CS68]. This method is analogous to completing the square for a quadratic polynomial. We use Cardano's method to determine if a cubic polynomial in $K[y]$ splits completely over K, where K is an arbitrary field of characteristic not equal to 2 or 3. Beginning with an arbitrary cubic polynomial in $K[y]$,

$$g(y) = ay^3 + by^2 + cy + d,$$

we divide through by the leading coefficient and perform a change of variables $y = x - b/3$ to eliminate the quadratic term, yielding a monic depressed cubic polynomial with coefficients in K,

$$f(x) = x^3 + Ax + B.$$

Note that since the transformations to depress the cubic simply shift the roots by $b/(3a)$, so g splits over K if and only if f splits over K.

Lemma 4 (Cardano [CS68]). *Let L be an algebraically closed field of characteristic not equal to 2 or 3, and let ζ be a primitive cube root of unity in L. Let $f(x) = x^3 + Ax + B \in L[x]$, and let $\Delta = B^2 + 4A^3/27$. If $A = 0$, let $C = -B$, and if $A \neq 0$, let C be either square root of Δ in L. Let u be a cube root of $(-B + C)/2$ and let $v = -A/(3u)$. Then the roots of f are $u + v$, $\zeta u + \zeta^2 v$, and $\zeta^2 u + \zeta v$.*

To determine when a cubic polynomial $f(x) \in \mathbb{Q}_p[x]$ splits completely over $\mathbb{Q}_p$, the method will depend on whether $\mathbb{Q}_p$ contains a primitive cube root of unity, which happens exactly when $p \equiv 1 \pmod 3$. Thus, we consider two cases: $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$.

2.3. ***Case* 1.** Suppose $p \equiv 1 \pmod 3$.

Theorem 5. *Let K be a field of characteristic not equal to 2 or 3, let L be an algebraic closure of K, and assume that K contains a primitive cube root of unity, ζ. Let $f(x) = x^3 + Ax + B \in K[x]$, and $\Delta = B^2 + 4A^3/27$. If $A = 0$, let $C = -B$, and if $A \neq 0$, let C be either square root of Δ in L. Then f splits completely over K if and only if*

(a) *Δ is a square in K, and*

(b) *$(-B + C)/2$ is a cube in K.*

Proof. Suppose $A = 0$. Then $\Delta = B^2$ is a square in K, so (a) is true. Additionally, $C = -B$ and $f(x) = x^3 + B$, which splits completely over K if and only if $-B$ is a cube in K, which happens exactly when (b) holds.

Now suppose $A \neq 0$. Let u be a cube root of $(-B + C)/2$ and let $v = -A/(3u)$. Let F be a Galois extension of K containing C and u.

Suppose the conditions (a) and (b) are met. By Lemma 4, the roots of f are $u + v$, $\zeta u + \zeta^2 v$, and $\zeta^2 u + \zeta v$ and thus f splits completely over K.

Conversely, suppose that f splits completely over K. Let $\sigma \in \mathrm{Gal}(L/K)$. Since σ fixes $u+v$ and $\zeta u + \zeta^2 v$,

$$u+v = \sigma(u)+\sigma(v) \quad \text{and} \quad \zeta u + \zeta^2 v = \zeta\sigma(u) + \zeta^2\sigma(v). \tag{1}$$

Note that $\left(\begin{smallmatrix} 1 & 1 \\ \zeta & \zeta^2 \end{smallmatrix}\right)$ has a nonzero determinant and thus

$$\begin{pmatrix} 1 & 1 \\ \zeta & \zeta^2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sigma(u)+\sigma(v) \\ \zeta\sigma(u)+\zeta^2\sigma(v) \end{pmatrix} \tag{2}$$

has a unique solution. By (1), $x = u$, $y = v$ is a solution to (2) and $x = \sigma(u)$, $y = \sigma(v)$ is a solution to (2) as well. Therefore $u = \sigma(u)$. By the Galois correspondence, $u \in K$, and thus (b) holds. Thus $u^3 = (-B+C)/2 \in K$. Since $C = 2u^3 + B$, $C \in K$ and therefore

$$\Delta = B^2 + 4A^3/27 = C^2$$

is a square in K, and (a) is true. □

Lemma 6. *Let p be a prime, $p \neq 3$, and let $a \in \mathbb{Z}_p$ with $|a|_p = 1$. Then a is a cube in $\mathbb{Q}_p$ if and only if $a \pmod p$ is a cube in $\mathbb{Z}_p/p\mathbb{Z}_p$.*

Proof. Suppose that a is a cube in $\mathbb{Z}_p$. Then a is a cube in $\mathbb{Z}_p/p\mathbb{Z}_p$ by the nature of quotient rings.

Conversely, suppose a_0 is a cube in $\mathbb{Z}/p\mathbb{Z}$ where $a_0 \equiv a \pmod p$, and let $b_0 \in \mathbb{Z}/p\mathbb{Z}$ satisfy $b_0^3 \equiv a_0 \pmod p$. Let $f(x) = x^3 - a$. Note that p does not divide 3 or b_0. By the strong triangle inequality,

$$|f(b_0)|_p = |b_0^3 - a|_p \leq \max\{|b_0^3 - a_0|_p, |a_0 - a|_p\} \leq \tfrac{1}{p}.$$

Further,

$$|f'(b_0)|_p = |3b_0^2|_p = 1.$$

By Hensel's lemma, a is a cube in $\mathbb{Q}_p$. □

Theorem 7. *Let p be a prime, with $p \equiv 1 \pmod 3$. Then the following algorithm yields $\tau_{3,p}$.*

(1) *Create a list, in ascending order of Mahler measure, of all irreducible, noncyclotomic cubic polynomials in $\mathbb{Z}[x]$ with Mahler measure bounded above by* 8.5. *Let $f(x)$ be the first polynomial on the list.*

(2) *Convert $f(x)$ into depressed form $g(x) = x^3 + Ax + B$ and let $\Delta = B^2 + 4A^3/27$.*

(3) *If Δ is not a square in $\mathbb{Q}_p$, return to step* (2) *with the next polynomial on the list.*

(4) *If $A = 0$, let $C = -B$, and otherwise let C be a square root of Δ in $\mathbb{Q}_p$. If $(-B+C)/2$ is not a cube in $\mathbb{Q}_p$, return to step* (2) *with the next polynomial on the list. Otherwise, terminate, giving $\tau_{3,p} = \frac{1}{3}\log M(f)$.*

Proof. Since $\tau_{3,p} \leq \tau_{3,p}^{\mathrm{ab}}$, by Theorem 3 we know that $\tau_{3,p} \leq 0.70376$. By [BG06, Proposition 1.6.7], a list of all polynomials with length less than 68 will contain all irreducible, noncyclotomic, cubic polynomials

with Mahler measure bounded above by 8.5. Any degree 3 algebraic number of height less than or equal to 0.70376 will be a root of a polynomial in the list. Thus, this algorithm will always terminate successfully.

Let f be the polynomial being considered. By Theorem 5, steps (3) and (4) will detect exactly when f splits completely over $\mathbb{Q}_p$. □

2.4. ***Case 2.*** Suppose $p \equiv 2 \pmod 3$.

Theorem 8. *Let K be a field of characteristic not equal to 2 or 3, K' be an algebraic closure of K, ζ be a primitive cube root of unity in K', and assume that $\zeta \notin K$. Let $f(x) = x^3 + Ax + B \in K[x]$ with $B \neq 0$ and let $\Delta = B^2 + 4A^3/27$. If $A = 0$, let $C = -B$, and if $A \neq 0$, let C be either square root of Δ in K'. Then f splits completely over K if and only if*

(a) *Δ is a square in $K(\zeta)$ and not a square in K, and*

(b) *$(-B + C)/2$ is a cube in $K(\zeta)$ and not a cube in K.*

Proof. Let u be a cube root of $(-B + C)/2$ and let $v = -A/(3u)$. By Lemma 4, the roots of f are $u + v$, $\zeta u + \zeta^2 v$, and $\zeta^2 u + \zeta v$.

We first suppose f splits completely in K. Let L be a Galois extension of K that contains u and ζ. Let $\sigma \in \mathrm{Gal}(L/K(\zeta))$. We want to show that σ must fix u. Since we are assuming that f splits completely over K, σ must fix $u + v$, $\zeta u + \zeta^2 v$, and $\zeta^2 u + \zeta v$,

$$u + v = \sigma(u) + \sigma(v), \tag{3}$$

$$\zeta^2 u + \zeta v = \zeta^2 \sigma(u) + \zeta \sigma(v). \tag{4}$$

By multiplying (3) by ζ and subtracting (4), we obtain

$$(\zeta - \zeta^2)u = (\zeta - \zeta^2)\sigma(u), \tag{5}$$

so $\sigma(u) = u$ because $\zeta \neq \zeta^2$. Thus, since all elements in $\mathrm{Gal}(L/K(\zeta))$ fix u, u must be in $K(\zeta)$.

It remains to show $u \notin K$. Let $\tau \in \mathrm{Gal}(L/K)$ be such that τ interchanges ζ and ζ^2. We now show that τ does not fix u. Since the roots of f must all be fixed by τ,

$$\zeta u + \zeta^2 v = \zeta^2 \tau(u) + \zeta \tau(v), \tag{6}$$

$$\zeta^2 u + \zeta v = \zeta \tau(u) + \zeta^2 \tau(v). \tag{7}$$

By multiplying (7) by ζ, and subtracting (6), we obtain

$$(1 - \zeta)u = (1 - \zeta)\tau(v) \tag{8}$$

and note that $\tau(v) = u$, so τ does not fix u. Thus $u \notin K$ and (b) holds.

Further, $u \in K(\zeta)$, so $u^3 = (-B + C)/2 \in K(\zeta)$, and thus Δ is a square in $K(\zeta)$ since $C \in K(\zeta)$. Since $K(u)$ is contained within $K(\zeta)$, a quadratic extension of K, and $u \notin K$, it follows that $[K(u) : K] = 2$. For sake of contradiction, suppose Δ is a square in K. Then $u^3 \in K$, so $[K(u) : K] = 3$ which is not true. Thus Δ is not a square in K, and (a) holds.

Conversely, suppose that (a) and (b) are true. Note that if $A = 0$, then Δ is a square in K, contradicting (a). Thus, $A \neq 0$. Let σ denote the nontrivial element of $\mathrm{Gal}(K(\zeta)/K)$. Since ζ and ζ^2 share a degree 2 minimal polynomial, σ must permute ζ and ζ^2.

By (a) and (b), $u, u^3 \notin K$ and $u, u^3 \in K(\zeta)$. Since u^3 and v^3 are the roots of $r(z) = z^2 + Bz - A^3/27$, we have $\sigma(u)^3 = \sigma(u^3) = v^3$. Therefore, either $\sigma(u) = v$, $\sigma(u) = \zeta v$, or $\sigma(u) = \zeta^2 v$.

We will now show that $\sigma(u) = v$ by eliminating the other two options by way of contradiction. We rely on the fact that elements of the Galois group send roots of f to roots of f, and that $\sigma^2(u) = u$. If $\sigma(u) = \zeta v$, then $u = \zeta^2\sigma(v)$, and $\sigma(u+v) = \sigma(u) + \sigma(v) = \zeta v + \zeta u$. Since $\zeta v + \zeta u$ is not a root of f, $\sigma(u) \neq \zeta v$. If $\sigma(u) = \zeta^2 v$, then $u = \zeta\sigma(v)$, and $\sigma(u+v) = \zeta^2 u + \zeta^2 v$. Since $\zeta^2 u + \zeta^2 v$ is not a root of f, $\sigma(u) \neq \zeta^2 v$.

Therefore, $\sigma(u) = v$ and $\sigma(v) = u$. Thus

$$\begin{aligned}\sigma(u+v) &= \sigma(u) + \sigma(v) = v + u,\\ \sigma(\zeta u + \zeta^2 v) &= \sigma(\zeta u) + \sigma(\zeta^2 v) = \zeta^2 v + \zeta u,\\ \sigma(\zeta^2 u + \zeta v) &= \sigma(\zeta^2 u) + \sigma(\zeta v) = \zeta v + \zeta^2 v.\end{aligned}$$

Since σ fixes the roots of f, f splits completely in K. □

Let $p \equiv 2 \pmod 3$. The third cyclotomic polynomial, $\Phi_3(x) = x^2 + x + 1$, has discriminant -3 and is the minimal polynomial for ζ. Since -3 is not a square in $\mathbb{Q}_p$, $\Phi_3(x)$ is irreducible over $\mathbb{Q}_p$, and thus $\mathbb{Q}_p$ does not contain a primitive cube root of unity. There are exactly three quadratic extensions of $\mathbb{Q}_p$: $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{-3})$, and $\mathbb{Q}_p(\sqrt{-3p})$. Let $K = \mathbb{Q}_p(\sqrt{-3}) = \mathbb{Q}_p(\zeta)$, the unique unramified quadratic extension of $\mathbb{Q}_p$. The p-adic absolute value on $\mathbb{Q}_p$ extends uniquely to $\mathbb{Q}_p(\sqrt{-3})$ by

$$|a + b\sqrt{-3}|_p = |N_{K/\mathbb{Q}_p}(a + b\sqrt{-3})|_p^{1/2} = |a^2 + 3b^2|_p^{1/2}.$$

The following three lemmas summarize some basic facts about this field.

Lemma 9. *Let $p \equiv 2 \pmod 3$, and $K = \mathbb{Q}_p(\sqrt{-3})$. For $x \in K^\times$, $|x|_p \in p^{\mathbb{Z}}$.*

Proof. Let $x = a + b\sqrt{-3}$, with $a, b \in \mathbb{Q}_p$ and $x \neq 0$. Suppose $|a|_p \neq |b|_p$. Then

$$|x|_p = |a^2 + 3b^2|_p^{1/2} = \max\{|a|_p, |b|_p\} \in p^{\mathbb{Z}}.$$

Suppose instead that $|a|_p = |b|_p = p^\ell$. Set $a_0 = p^\ell a$ and $b_0 = p^\ell b$. Note that since $|a_0|_p = |b_0|_p = 1$, we have $|a_0|_p, |b_0|_p \in p^{\mathbb{Z}}$. Thus,

$$|a_0^2 + 3b_0^2|_p \leq \max\{1, |3|_p\} \leq 1.$$

Suppose, for the sake of contradiction, that $|a_0^2 + 3b_0^2|_p < 1$. Then we have that $a_0^2 + 3b_0^2 \equiv 0 \pmod p$, which is a contradiction since -3 is not a quadratic residue modulo p. Thus

$$|x|_p = |a^2 + 3b^2|_p^{1/2} = |p^{-2\ell}(a_0^2 + 3b_0^2)|_p^{1/2} = p^\ell |a_0^2 + 3b_0^2|_p^{1/2} = p^\ell \in p^{\mathbb{Z}}.$$ □

Lemma 10. *Let p be a prime with $p \equiv 2 \pmod 3$, $K = \mathbb{Q}_p(\sqrt{-3})$, and $C \in K$. Let $k \in \mathbb{N}$, $p \nmid k$. Then $f(x) = x^k - C$ has a root in K if and only if*

(a) *$|C|_p = p^{k\ell}$ for some $l \in \mathbb{Z}$, and*

(b) *$p^{k\ell}C \pmod p$ is a k-th power in $\mathbb{Z}_p[\sqrt{-3}]/(p)$.*

Proof. First we assume the existence of $r \in K$ so that $f(r) = 0$, and verify that (a) and (b) hold. By Lemma 9, $|r|_p = p^\ell$ for some $\ell \in \mathbb{Z}$. Since

$$|C|_p = |r^k|_p = p^{k\ell},$$

(a) is true. Further,

$$p^{kl}C = p^{kl}r^k = (p^l r)^k$$

and thus $p^{kl}C$ is the k-th power of $p^l r \pmod p$ in $\mathbb{Z}[\sqrt{-3}]$, and therefore also holds after reduction modulo (p).

Conversely, we suppose $C \in \mathbb{Q}_p(\sqrt{-3})$ satisfies conditions (a) and (b), and show that C is a k-th power in K. Replacing C with $p^{kl}C$, without loss of generality we may assume $|C|_p = 1$. By condition (b), there exists $a + b\sqrt{-3} \in \mathbb{Z}_p[\sqrt{-3}]/(p)$, where $a, b \in \{0, 1, 2, \ldots, p-1\}$ and $C \equiv (a + b\sqrt{-3})^k \pmod p$. Then

$$|f(a + b\sqrt{-3})|_p = |(a + b\sqrt{-3})^k - C|_p \leq \tfrac{1}{p},$$
$$|f'(a + b\sqrt{-3})|_p = |k(a + b\sqrt{-3})^{k-1}|_p = 1.$$

Thus, by Hensel's lemma f has a root in K. □

Lemma 11. *Let p be a prime with $p \equiv 2 \pmod 3$, and $K = \mathbb{Q}_p(\sqrt{-3})$. Let $x \in \mathbb{Q}_p$ be nonzero and the square of an element in K. Then exactly one of the following two cases is true*:

(a) *$x = a^2$ for some $a \in \mathbb{Q}_p$.*

(b) *$x = -3b^2$ for some $b \in \mathbb{Q}_p$.*

Proof. Suppose $x = (a + b\sqrt{-3})^2$ for $a, b \in \mathbb{Q}_p$. Then

$$x = a^2 - 3b^2 + 2ab\sqrt{-3}.$$

Since $\sqrt{-3} \notin \mathbb{Q}_p$, we have $ab = 0$. If $a = 0$, then $x = -3b^2$ and (b) holds. If $b = 0$, then $x = a^2$ and (a) holds. □

The previous lemma gives us the machinery to detect and solve for a square root in K, since x is a square in K and not in $\mathbb{Q}_p$ if and only if $x/(-3) = b^2$ for some $b \in \mathbb{Q}_p$.

Theorem 12. *Let p be an odd prime, with $p \equiv 2 \pmod 3$. Then the following algorithm yields $\tau_{3,p}$.*

(1) *Create a list, in ascending order of Mahler measure, of all irreducible, noncyclotomic cubic polynomials in $\mathbb{Z}[x]$ with Mahler measure less than* 8.5. *Let $f(x)$ be the first polynomial on the list.*

(2) *Convert $f(x)$ into depressed form $g(x) = x^3 + Ax + B$ and let $\Delta = B^2 + 4A^3/27$.*

(3) *If Δ is a square in $\mathbb{Q}_p$ or is not a square in $\mathbb{Q}_p(\sqrt{-3})$, return to step* (2) *with the next polynomial on the list.*

(4) *If $A = 0$, let $C = -B$, and otherwise let C be a square root of Δ in $\mathbb{Q}_p(\sqrt{-3})$. If $(-B+C)/2$ is not a cube in $\mathbb{Q}_p(\sqrt{-3})$, return to step* (2) *with the next polynomial on the list.*

(5) *If $(-B+C)/2$ is a cube in $\mathbb{Q}_p$, return to step* (2) *with the next polynomial on the list. Otherwise, terminate, giving $\tau_{3,p} = \frac{1}{3}\log M(f)$.*

Proof. Since $\tau_{3,p} \leq \tau_{3,p}^{\text{ab}}$, by Theorem 3 we know that $\tau_{3,p} \leq 0.70376$. By [BG06, Proposition 1.6.7], a list of all polynomials with length less than 68 will contain all irreducible, noncyclotomic, cubic polynomials with Mahler measure bounded above by 8.5. Any degree 3 algebraic number of height less than or equal to 0.70376 will be a root of a polynomial in the list. Thus, this algorithm will always terminate successfully.

Let f be the polynomial being considered. By Theorem 8, steps (3), (4), and (5) will detect exactly when f splits completely over $\mathbb{Q}_p$. □

2.5. ***Implementation.*** The function `is_cube_in_k` checks to see whether $A + B\sqrt{-3}$ is a cube in $K = \mathbb{Q}_p(\sqrt{-3})$ by applying Lemma 10.

```
def is_cube_in_k(A,B,p):
    A = K(A);
    B = K(B);
    AA = A.list();
    BB = B.list();
    A0 = AA[0];
    B0 = BB[0];
    if A.abs()<1:
        A0 = 0
    if B.abs()<1:
        B0 = 0
    for c in [0..p-1]:
        for d in [0..p-1]:
            if (c*c*c - 9*c*d*d)%p==A0:
                if (3*c*c*d - 3*d*d*d)%p==B0:
                    return True
    return False
```

The function `is_cube_in_Qp` checks to see if A is a cube in $\mathbb{Q}_p$ by applying Lemma 6.

```
def is_cube_in_Qp(A,p):
    val = A.ordp();
    if 3.divides(val)==True:
        L = A.expansion();
        a = L[0];
        if IsCubeInFp(a,p)==True:
            return True;
    return False
```

The function `tau_dp_1mod3` determines $\tau_{3,p}$ for the prime p where $p \equiv 1 \pmod 3$, by implementing the algorithm described in Theorem 7. Recall the array `Polynomials` contains the contents of the file `irred_polynomials_L68`, which has L entries. These were calculated in Section 2.1.

```
def tau_dp_1mod3(p):
    i = 0;
    while i < L-1:
        A = Polynomials[i][5];
        B = Polynomials[i][6];
        D = Polynomials[i][7];
        A = K(A);
        B = K(B);
        D = K(D);
        if QQ(D).is_padic_square(p)==True:
            if A==0:
                C = -B;
            if A!=0:
                C = D.square_root();
            Check = (C - B) / 2;
            if is_cube_in_Qp(Check,p)==True:
                return Polynomials[i]
        i = i + 1;
    return False
```

The function tau_dp_2mod3 determines $\tau_{3,p}$ for the prime p where $p \equiv 2 \pmod 3$, by implementing the algorithm described in Theorem 12.

```
def tau_dp_2mod3(p):
    i = 0;
    while i < L-1:
        D = Polynomials[i][7];
        if D.is_padic_square(p)==False:
            b = D / (-3);
            if b.is_padic_square(p)==True:
                a = - Polynomials[i][6] / 2;
                b = K(b);
                b = sqrt(b) / 2;
                if is_cube_in_k(a,b,p)==True:
                    return Polynomials[i]
        i=i+1;
    return False
```

The following code determines $\tau_{3,p}$ for all primes p greater than 5, up to and including the N-th prime.

```
Polynomials=load('irred_polynomials_L68')
L=len(Polynomials)
P=Primes(); # P is now a list of all primes
N=25
rows = [['P', '$\tau_{3,p}$', 'Polynomial']]
for i in[2..N]:
    p = P.unrank(i);
    K = Qp(p, prec = 6, type = 'capped-rel', print_mode = 'series');
    if p%3==1:
        tdp = tau_dp_1mod3(p)
        Poly = tdp[1]*x^3 + tdp[2]*x^2 + tdp[3]*x + tdp[4];
        h = tdp[8].n(digits=5);
        rows.append([p,h,Poly])
    if p%3==2:
        tdp = tau_dp_2mod3(p)
        Poly = tdp[1]*x^3 + tdp[2]*x^2 + tdp[3]*x +tdp[4];
        h = tdp[8].n(digits=5);
        rows.append([p,h,Poly])
```

3. Results

Table 2 contains some values for $\tau_{3,p}$.

p	$\tau_{3,p}$	f_α
5	0.36620	x^3-2x^2-x-3
7	0.30387	$2x^3-2x^2+x-2$
11	0.36620	x^3-x^2-2x-3
13	0.26986	x^3-2x^2-x+1
17	0.23105	x^3-x^2-x+2
19	0.23105	x^3-x^2-2
23	0.23105	x^3-x^2+x-2
29	0.26986	x^3-2x^2-x+1
31	0.23105	x^3-x-2
37	0.27319	x^3-x^2-2x-2
41	0.23105	x^3-x^2+x-2
43	0.23105	x^3-2
47	0.12741	x^3-x^2-1
53	0.20313	x^3-x^2-x-1
59	0.093733	x^3-x^2+1
61	0.28206	$2x^3-x^2+2$
67	0.12741	x^3-x^2-1
71	0.23105	x^3-x^2-x+2
73	0.29111	$2x^3-x^2-2$
79	0.28612	x^3-2x^2-2
83	0.23105	x^3-2x-2
89	0.27535	$2x^3-2x^2-x+2$
97	0.26986	x^3-2x^2-x+1
101	0.093733	x^3-x^2+1
103	0.20313	x^3-x^2-x-1
107	0.23105	x^3-x-2
109	0.23105	x^3-2
113	0.23105	x^3-x-2
127	0.23105	x^3-x^2-2
131	0.12741	x^3-x^2-1
137	0.30697	x^3-x^2-3x-2
139	0.23105	x^3-x^2-x+2
149	0.12741	x^3-x^2-1
151	0.28206	$2x^3-x^2+2$
157	0.23105	x^3-2x-2
163	0.20313	x^3-x^2-x-1
167	0.093733	x^3-x^2+1
173	0.093733	x^3-x^2+1
179	0.27319	x^3-x^2-2x-2
181	0.26986	x^3-2x^2-x+1
191	0.23105	x^3-x^2-2
193	0.23105	x^3-x^2+x-2
197	0.23105	x^3-x^2-x+2
199	0.20313	x^3-x^2-x-1
211	0.093733	x^3-x^2+1
223	0.093733	x^3-x^2+1
227	0.12741	x^3-x^2-1
229	0.23105	x^3-x^2+x-2
233	0.27319	x^3-x^2-2x-2
239	0.26986	x^3-2x^2-x+1
241	0.30697	x^3-x^2-3x-2
251	0.23105	x^3-x-2
257	0.20313	x^3-x^2-x-1
263	0.27319	x^3-x^2-2x-2
269	0.20313	x^3-x^2-x-1
271	0.093733	x^3-x^2+1
277	0.23105	x^3-x^2-2
281	0.26986	x^3-2x^2-x+1
283	0.12741	x^3-x^2-1
293	0.12741	x^3-x^2-1
307	0.093733	x^3-x^2+1
311	0.20313	x^3-x^2-x-1
313	0.23105	x^3-2x-2
317	0.093733	x^3-x^2+1
331	0.28206	$2x^3-x^2+2$
337	0.26986	x^3-2x^2-x+1
347	0.093733	x^3-x^2+1
349	0.12741	x^3-x^2-1
353	0.23105	x^3-x^2-2
359	0.23105	x^3-x-2
367	0.23105	x^3-x^2-2
373	0.23105	x^3-x^2-x+2
379	0.12741	x^3-x^2-1
383	0.23105	x^3-x^2-x+2
389	0.23105	x^3-x^2-x+2
397	0.20313	x^3-x^2-x-1
401	0.20313	x^3-x^2-x-1
409	0.30387	$2x^3-2x^2+x-2$
419	0.20313	x^3-x^2-x-1
421	0.20313	x^3-x^2-x-1
431	0.12741	x^3-x^2-1
433	0.23105	x^3-2
439	0.23105	x^3-x^2-x+2
443	0.23105	x^3-x^2-2

Table 2. Some values for $\tau_{3,p}$.

4. Conclusion and future work

In this paper we relied on the fact that we can determine that a finite list of polynomials is guaranteed to contain one that splits over $\mathbb{Q}_p$ for any prime p. We restricted our search to cubic numbers that exist in abelian extensions of $\mathbb{Q}$ to prove this. Moving forward, we will determine that we can guarantee that for any degree d, there is some $N_d \in \mathbb{Z}$ such that $\tau_{d,p}^{\mathrm{ab}}$ depends only on $p \pmod{N_d}$. For example, $N_2 = 5$ and $N_3 = 228979643050431$.

When we look at the small nonzero values attained by the height function on cubic numbers, we see that the smallest value is 0.093733. It would be interesting to classify all primes such that $\tau_{3,p} = 0.093733$.

References

[Bak06] Matt Baker. Algebraic number theory course notes (fall 2006) Math 8803, Georgia Tech. Available at people.math.gatech.edu/∼mbaker/pdf/ANTBook.pdf, 2006. Accessed: 2017-12-31.

[BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine Geometry*. Number 4 in New Mathematical Monographs. Cambridge University Press, 2006.

[BZ01] Enrico Bombieri and Umberto Zannier. A note on heights in certain infinite extensions of $\mathbb{Q}$. *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni*, 12(1):5–14, 2001.

[Cas86] John William Scott Cassels. *Local fields*, volume 3. Cambridge University Press, 1986.

[Con18] Keith Conrad. Galois groups of cubics and quartics (not in characteristic 2). Available at http://www.math.uconn.edu/∼kconrad/blurbs/galoistheory/cubicquartic.pdf, 2018. Accessed: 2018-06-14.

[CS68] Girolamo Cardano and C Spon. Ars magna (1545). *Opera Omnia*, 4:221–302, 1968.

[Has30] Helmut Hasse. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. *Math. Z.*, 31(1):565–582, 1930.

[HS93] Gerald Höhn and Nils Peter Skoruppa. Un résultat de Schinzel. *J. Théor. Nombres Bordeaux*, 5(1):185, 1993.

[Pet] Clayton Petsche. The height of algebraic units in local fields.

[Pot18] Lukas Pottmeyer. Small totally p-adic algebraic numbers. 2018 arXiv:1802.05923

[PS19] Clayton Petsche and Emerald Stacy. A dynamical construction of small totally p-adic algebraic numbers. *J. of Number Theory*, 202:27–36, 2019.

[Sch75] Andrzej Schinzel. Addendum to the paper "On the product of the conjugates outside the unit circle of an algebraic number". *Acta Arithmetica*, 26:329–331, 1975.

[Smy80] Chris Smyth. On the measure of totally real algebraic integers. *J. of the Australian Math. Soc.*, 30(2):137–149, 1980.

Received 23 Feb 2020. Revised 1 Aug 2020.

EMERALD STACY: estacy2@washcoll.edu
Mathematics and Computer Science, Washington College, Chestertown, MD, United States

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

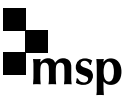
Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.



MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS