Canad. J. Math. Vol. **67** (5), 2015 pp. 1046–1064
http://dx.doi.org/10.4153/CJM-2015-021-2

Explicit Form of Cassels' p-adic Embedding Theorem for Number Fields

Arturas Dubickas, Min Sha, and Igor Shparlinski

Abstract. In this paper, we give a general explicit form of Cassels' p-adic embedding theorem for number fields. We also give its refined form in the case of cyclotomic fields. As a byproduct, given an irreducible polynomial f over $\mathbb{Z}$, we give a general unconditional upper bound for the smallest prime number p such that f has a simple root modulo p.

1 Introduction

1.1 Motivation

We start by recalling a result of Cassels [4] that gives a p-adic embedding for finitely generated fields of characteristic 0, which we reproduce here for the convenience of the reader.

Theorem 1.1 *Let K be a finitely generated extension of the rational field $\mathbb{Q}$, and let S be a finite set of non-zero elements of K. Then there exist infinitely many primes p such that there is an embedding*

$$\sigma\colon K \hookrightarrow \mathbb{Q}_p \tag{1.1}$$

of K into the field of p-adic numbers $\mathbb{Q}_p$ for which $|\sigma(\beta)|_p = 1$ for all $\beta \in S$, where $|\cdot|_p$ denotes the p-adic valuation.

Theorem 1.1 is often a useful tool when one needs to employ p-adic techniques to solve various problems in number fields. The point is that for many natural problems over general fields of characteristic zero, one can expect to get a result that is not worse than the corresponding one in the case of an algebraic number field, or even in the case of the field of rational numbers. For example, the above theorem has been used for a long time in the study of recurrence sequences over number fields; see, for example, [5, 10, 14–16].

Received by the editors February 19, 2014; revised February 23, 2015.
Published electronically July 13, 2015.
The research of A. D. was supported by the Research Council of Lithuania Grant MIP-068/2013/LSS-110000-740. The research of M. S. and I. E. S. was supported by Australian Research Council Grant DP130100237.
AMS subject classification: **11R04**, 11S85, 11G50, 11R09, 11R18.
Keywords: number field, p-adic embedding, height, polynomial, cyclotomic field.

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

1.2 Main Results

In this paper, we supplement the methods of Cassels [4] with several new ingredients and give an explicit version of Theorem 1.1 in the case when K is a number field. We believe these new ingredients can be of independent interest and may find several other applications.

To begin with, we state the following general theorem and several subsequent corollaries. Throughout the paper, for an algebraic number $\alpha \in \overline{\mathbb{Q}}$, we denote its (Weil) absolute logarithmic height by $\mathrm{h}(\alpha)$. For an integer $m \geq 1$, we define $\log^+ m = \max\{1, \log m\}$, so that $\log^+ m = \log m$ for all $m \geq 3$.

Theorem 1.2 *Let K be a number field of degree $d \geq 2$ generated by $\alpha_1, \dots, \alpha_m \in K \smallsetminus \mathbb{Q}$ over $\mathbb{Q}$, and let $\beta_1, \dots, \beta_n$ be some fixed non-zero elements of K. Then there exists a prime number p satisfying*

$$p \leq m^d \exp\Big(d \sum_{i=1}^{m} \mathrm{h}(\alpha_i) \Big) \Big(dn \sum_{i=1}^{m} \mathrm{h}(\alpha_i) + d \sum_{i=1}^{n} \mathrm{h}(\beta_i) + dn \log^+ m \Big)^{O(d^2)}$$

such that (1.1) holds and $|\sigma(\beta_i)|_p = 1$, for $1 \leq i \leq n$.

Corollary 1.3 *Let K be a number field of degree $d \geq 2$ generated by $\alpha_1, \dots, \alpha_m \in K \smallsetminus \mathbb{Q}$ over $\mathbb{Q}$. Then there exists a prime number p satisfying*

$$p \leq \exp\Big(d \sum_{i=1}^{m} \mathrm{h}(\alpha_i) \Big) \Big(dm \sum_{i=1}^{m} \mathrm{h}(\alpha_i) + dm \Big)^{O(d^2)},$$

such that (1.1) holds and $|\sigma(\alpha_i)|_p = 1$, for $1 \leq i \leq m$.

Corollary 1.4 *Let K be a number field of degree $d \geq 2$ generated by an algebraic integer α over $\mathbb{Q}$, and let $\beta_1, \dots, \beta_n \in \mathbb{Z}[\alpha]$ be some fixed non-zero algebraic integers (respectively, units) of K. Then there exists a prime number p satisfying*

$$p \leq \exp(d\mathrm{h}(\alpha)) \big(d\mathrm{h}(\alpha) + d \big)^{O(d^2)}$$

such that (1.1) holds and $|\sigma(\beta_i)|_p \leq 1$ (resp., $|\sigma(\beta_i)|_p = 1$), for $1 \leq i \leq n$.

The above results depend on the generators we choose for K over $\mathbb{Q}$. In contrast, the following bound is independent of the choice of generators, but involves the discriminant of K.

Corollary 1.5 *Let K be a number field of degree $d \geq 2$ with discriminant D_K, and let $\beta_1, \dots, \beta_n$ be some fixed non-zero elements of K. Furthermore, suppose that K has at least one real embedding. Then there exists a prime number p satisfying*

$$p \leq \sqrt{|D_K|} \Big(n \log |D_K| + d \sum_{i=1}^{n} \mathrm{h}(\beta_i) \Big)^{O(d^2)},$$

such that (1.1) holds and $|\sigma(\beta_i)|_p = 1$, for $1 \leq i \leq n$.

For a prime number ℓ and an integer m, we write, as usual, $\ell^e \| m$ if e is the largest integer with $\ell^e \mid m$.

Given an integer $m \geq 2$, suppose that $\ell = P(m)$, where $P(m)$ denotes the largest prime divisor of m and $\ell^e \| m$. Define

$$\delta(m) = \begin{cases} \phi(m/\ell^e) & \text{if } \ell \equiv 1 \pmod{m/\ell^e}, \\ 1 & \text{otherwise,} \end{cases}$$

where ϕ is Euler's totient function. In particular, $\delta(m) = 1$ if m is a power of a prime or $m \geq \ell^{e+1}$.

For cyclotomic fields, we can get a refined explicit form of Theorem 1.1.

Theorem 1.6 *Let K be the m-th cyclotomic field with $m > 2$, and let $\beta_1, \dots, \beta_n$ be some fixed non-zero elements of K. Then there exists a prime number p satisfying*

$$p \leq \Big(d \sum_{i=1}^{n} \mathrm{h}(\beta_i) + dn \Big)^{O(d\delta(m))},$$

where $d = \phi(m)$, such that (1.1) holds and $|\sigma(\beta_i)|_p = 1$ for $1 \leq i \leq n$.

1.3 Approach

To prove Theorems 1.2 and 1.6 we follow, roughly speaking, the original proof of Cassels and make each step there explicit. For our purpose, we need to tackle the following three subproblems that appear to be new and contain the main techniques in this paper. We believe that these problems and our contribution to them can be of independent interest.

First, given generators $\alpha_1, \dots, \alpha_m$ of K over $\mathbb{Q}$, we need to construct a primitive element α of K such that $\mathrm{h}(\alpha)$ can be bounded explicitly in terms of heights $\mathrm{h}(\alpha_i)$, $1 \leq i \leq m$, and $[K:\mathbb{Q}]$. We study this problem much more than what we need in our particular application in Section 2.

Second, given a primitive element α of K and an arbitrary element β, β can be expressed uniquely as a linear combination of the basis $\{1, \alpha, \dots, \alpha^{d-1}\}$. We need to bound the heights of the coefficients explicitly. This is handled in Section 3.

Third, given an arbitrary irreducible polynomial f over $\mathbb{Z}$, we need to derive an upper bound for the smallest prime p such that f has a simple root modulo p. We study this problem extensively by using elementary arguments in Section 4.

Now, we give a brief outline of the proof of Theorem 1.2. We first construct a primitive element α of K with bounded height from the given generators $\alpha_1, \dots, \alpha_m$. Let f be the minimal polynomial of α over $\mathbb{Z}$. Put $\beta_{n+i} = \beta_i^{-1}$ for $1 \leq i \leq n$. Then, for $1 \leq i \leq 2n$, we express β_i as a linear combination of the basis $\{1, \alpha, \dots, \alpha^{d-1}\}$ such that all the coefficients are in reduced form, and denote by b_i the least common multiple of the denominators of the coefficients. Note that a prime p is suitable if it satisfies the following two conditions:

- f has a simple root modulo p.
- p does not divide any b_i, $1 \leq i \leq 2n$.

Using the results and techniques developed in solving the above three subproblems, we derive an upper bound for the smallest such prime p; see Section 5 for more details.

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

Throughout the paper, we use the Landau symbols O and o. Recall that the assertion $U = O(V)$ is equivalent to the inequality $|U| \le cV$ with some constant c, while $U = o(V)$ means that $U/V \to 0$.

2 "Height" of a Number Field

2.1 Definitions and Main Results

Let K be a number field generated by $\alpha_1, \alpha_2, \dots, \alpha_m$ over $\mathbb{Q}$. In this section, we show the existence of a primitive element α of K of small height. We present more general versions than we actually need for our purpose.

Given a polynomial $f(x) = a_d x^d + \dots + a_0 = a_d(x-\alpha_1)\cdots(x-\alpha_d) \in \mathbb{C}[x]$, where $a_d \ne 0$, its *height* is defined by $H(f) = \max_{0\le i\le d} |a_i|$, and its *Mahler measure* by

$$M(f) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

For each $f \in \mathbb{C}[x]$ of degree d, these quantities are related by the following inequality

$$H(f)2^{-d} \le M(f) \le H(f)\sqrt{d+1}. \tag{2.1}$$

The left inequality of (2.1) follows from the identity

$$a_{d-i} = (-1)^i a_d \sum_{1\le j_1<\dots<j_i\le d} \alpha_{j_1}\cdots\alpha_{j_i},$$

since each product $|a_d\alpha_{j_1}\cdots\alpha_{j_i}|$ does not exceed $M(f)$ (see, *e.g.*, [20, Lemma 3.11]). The right inequality of (2.1) follows from the so-called Landau inequality $M(f) \le \left(\sum_{i=0}^{d}|a_i|^2\right)^{\frac{1}{2}}$, which was proved, for instance, in [3], [9] and [17].

For an algebraic number $\alpha \in \overline{\mathbb{Q}}$ of degree d, its Mahler measure $M(\alpha)$ is the Mahler measure of its minimal polynomial f over $\mathbb{Z}$, that is, $M(\alpha) = M(f)$. Then the *(Weil) absolute logarithmic height* $\mathrm{h}(\alpha)$ of α is equal to $d^{-1}\log M(\alpha)$. We also define the usual *height* $H(\alpha)$ of α as the height of f, namely, $H(\alpha) = H(f)$.

Theorem 2.1 *Let $\alpha_1, \dots, \alpha_m$ be some algebraic numbers of degree $d_1, \dots, d_m \ge 2$, respectively, and let $K = \mathbb{Q}(\alpha_1, \dots, \alpha_m)$ be of degree d over $\mathbb{Q}$. Then K contains an algebraic number α satisfying $K = \mathbb{Q}(\alpha)$ and such that*

$$\mathrm{h}(\alpha) \le \log(m\lfloor d/2\rfloor) + \mathrm{h}(\alpha_1) + \dots + \mathrm{h}(\alpha_m).$$

Equivalently, the bound of Theorem 2.1 can be written as

$$M(\alpha) \le (m\lfloor d/2\rfloor)^d \prod_{i=1}^{m} M(\alpha_i)^{d/d_i}.$$

Corollary 2.2 *Let $\alpha_1, \dots, \alpha_m$ be some algebraic numbers of degree $d_1, \dots, d_m \ge 2$ and usual height $H_1, \dots, H_m$, respectively, and let $K = \mathbb{Q}(\alpha_1, \dots, \alpha_m)$ be of degree d over $\mathbb{Q}$. Then K contains an algebraic number α satisfying $K = \mathbb{Q}(\alpha)$ and*

$$H(\alpha) \le (md)^d \prod_{i=1}^{m} (d_i+1)^{d/(2d_i)} \prod_{i=1}^{m} H_i^{d/d_i}.$$

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

Corollary 2.3 *Let $f \in \mathbb{Z}[x]$ be a polynomial of degree d with height H whose splitting field K is of degree D over $\mathbb{Q}$. Then for some algebraic number α satisfying $K = \mathbb{Q}(\alpha)$, we have*

$$\mathrm{h}(\alpha) \le \log\big((d-1)\lfloor D/2\rfloor\big) + \frac{d-1}{d}\log(H\sqrt{d+1}),$$

and

$$H(\alpha) \le (d-1)^D D^D (d+1)^{(d-1)D/(2d)} H^{(d-1)D/d}.$$

2.2 Preparations

To prove the above results, we use the following two known facts.

Lemma 2.4 *Let K be a separable extension of degree $d > 1$ of a field F. Suppose $K = F(\alpha_1, \dots, \alpha_m)$. Then, for any finite subset S of F, there are at least $|S|^{m-1}(|S|-d+1)$ m-tuples $(b_1, \dots, b_m) \in S^m$ for which the element $\alpha = b_1\alpha_1 + \cdots + b_m\alpha_m$ is primitive for K over F, namely, $K = F(\alpha)$.*

Lemma 2.5 *Let $f \in \mathbb{Z}[x_1, \dots, x_m]$ be a non-zero polynomial in m variables. Then, for any algebraic numbers $\gamma_1, \dots, \gamma_m$, we have*

$$\mathrm{h}(f(\gamma_1, \dots, \gamma_m)) \le \log L(f) + \sum_{i=1}^{m} \mathrm{h}(\gamma_i) \deg_{x_i} f,$$

where $\deg_{x_i} f$ is the partial degree of f, and $L(f)$ is the sum of moduli of the coefficients of f.

Lemma 2.4 is the main result of [2] (see also [22, Lemma 3.3] for a slightly weaker result), whereas Lemma 2.5 is exactly [20, Lemma 3.7].

2.3 Proofs

Proof of Theorem 2.1 We apply Lemma 2.4 to

$$F = \mathbb{Q} \quad \text{and} \quad S = \big\{-\lfloor d/2\rfloor, \dots, \lfloor d/2\rfloor\big\}$$

(note that $d > 1$). Since $|S| = 2\lfloor d/2\rfloor + 1 \ge d$, the number $|S|^{m-1}(|S| - d + 1) \ge |S|^{m-1}$ is positive. Thus, there are some m (not necessarily distinct) integers $b_1, \dots, b_m \in S$ such that the element $\alpha = b_1\alpha_1 + \cdots + b_m\alpha_m$ satisfies $K = \mathbb{Q}(\alpha)$. Applying Lemma 2.5 to the polynomial $f(x_1, \dots, x_m) = b_1x_1 + \cdots + b_mx_m$ of length $L(f) = |b_1| + \cdots + |b_m| \le m\lfloor d/2\rfloor$, with $\gamma_1 = \alpha_1, \dots, \gamma_m = \alpha_m$, we deduce

$$\begin{aligned}\frac{\log M(\alpha)}{d} = \mathrm{h}(\alpha) = \mathrm{h}\big(f(\alpha_1, \dots, \alpha_m)\big) &\le \log\big(m\lfloor d/2\rfloor\big) + \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_m)\\ &= \log\big(m\lfloor d/2\rfloor\big) + \log\Big(\prod_{i=1}^{m} M(\alpha_i)^{1/d_i}\Big).\end{aligned}$$

This implies the required inequalities of Theorem 2.1. ∎

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

Proof of Corollary 2.2 Note that by the right inequality of (2.1), we have $M(\alpha_i) \le H_i\sqrt{d_i+1}$ for $i = 1, \dots, m$. Thus,

$$\prod_{i=1}^{m} M(\alpha_i)^{d/d_i} \le \prod_{i=1}^{m} H_i^{d/d_i} \prod_{i=1}^{m} (d_i+1)^{d/(2d_i)}.$$

Now, selecting α as in Theorem 2.1, we have $\deg \alpha = d$. Hence, by the left inequality of (2.1) and Theorem 2.1, we obtain

$$H(\alpha) \le 2^d M(\alpha) \le (md)^d \prod_{i=1}^{m} M(\alpha_i)^{d/d_i} \le (md)^d \prod_{i=1}^{m} (d_i+1)^{d/(2d_i)} \prod_{i=1}^{m} H_i^{d/d_i},$$

as claimed. ■

Proof of Corollary 2.3 Write the polynomial $f \in \mathbb{Z}[x]$ in the form $f = f_0 f_1^{n_1} \cdots f_q^{n_q}$, where $f_1, \dots, f_q \in \mathbb{Z}[x]$ are distinct irreducible polynomials of degrees $d_1, \dots, d_q \ge 2$, respectively, and $f_0 \in \mathbb{Z}[x]$ is a product of linear polynomials. Assume that $q \ge 1$, since the claim is trivial otherwise, by taking $\alpha = 1$. Thus, $D > 1$. Furthermore, in view of

$$d = n_1 d_1 + \cdots + n_q d_q + \deg f_0,$$

we have $d_i \le d$ for each $i = 1, \dots, q$.

Put $m = d_1 - 1 + \cdots + d_q - 1$. It is clear that the splitting field K of f is generated by arbitrary $d_1 - 1$ roots of f_1, arbitrary $d_2 - 1$ roots of $f_2, \dots,$ arbitrary $d_q - 1$ roots of f_q. By Theorem 2.1, there is an algebraic number $\alpha \in K$ satisfying $K = \mathbb{Q}(\alpha)$ and

$$M(\alpha) \le (m\lfloor D/2 \rfloor)^D \prod_{i=1}^{q} M(f_i)^{(d_i-1)D/d_i},$$

since we have $d_i - 1$ copies of $M(f_i)$ for each $i = 1, \dots, q$. Using $(d_i - 1)/d_i \le (d-1)/d$ (which follows from $d_i \le d$) and

$$M(f_1) \cdots M(f_q) = M(f_1 \cdots f_q) \le M(f_1 \cdots f_q) M(f_0 f_1^{n_1-1} \cdots f_q^{n_q-1}) = M(f)$$

(which follows from the multiplicativity of the Mahler measure and $M(f_i) \ge 1$), we find that

$$M(\alpha) \le \big(m\lfloor D/2 \rfloor\big)^D M(f)^{(d-1)D/d}.$$

Note that $m \le d-1$, and by the right inequality of (2.1), $M(f) \le H(f)\sqrt{d+1} = H\sqrt{d+1}$. Therefore, using these estimates and applying the left inequality of (2.1), we find that

$$\begin{aligned} \mathrm{h}(\alpha) = \frac{\log M(\alpha)}{D} &\le \log\big(m\lfloor D/2 \rfloor\big) + \frac{d-1}{d} \log(M(f)) \\ &\le \log\big((d-1)\lfloor D/2 \rfloor\big) + \frac{d-1}{d} \log(H\sqrt{d+1}), \end{aligned}$$

and

$$\begin{aligned} H(\alpha) &\le 2^D M(\alpha) \le (mD)^D M(f)^{(d-1)D/d} \\ &\le \big(((d-1)D)^D (H\sqrt{d+1}\big)^{(d-1)D/d} \\ &= (d-1)^D D^D (d+1)^{(d-1)D/(2d)} H^{(d-1)D/d}, \end{aligned}$$

as claimed. ■

3 Bounding the Heights of Coefficients

3.1 Main Result

Let L/K be a number field extension of degree $d \geq 2$, and let $L = K(\alpha)$. Then, for any non-zero $\beta \in L$, there exist some $a_0, a_1, \dots, a_{d-1} \in K$ such that

$$\beta = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}.$$

Now, we bound the height of each coefficient a_i, $0 \leq i \leq d-1$, as follows.

Theorem 3.1 *Let L/K be a number field extension of degree $d \geq 2$, and $L = K(\alpha)$. Given non-zero $\beta \in L$, and $a_0, a_1, \dots, a_{d-1} \in K$, such that*

$$\beta = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1},$$

we have

$$\mathrm{h}(a_i) \leq d\mathrm{h}(\beta) + 3d(d-1)\mathrm{h}(\alpha) + d\log\binom{d-1}{i} + d(d-1)\log 2 + \log d,$$

for $i = 0, 1, \dots, d-1$.

Note that since we have

$$\binom{d-1}{i} \leq 2^{d-1}, \qquad i = 0, 1, \dots, d-1$$

for the binomial coefficients, Theorem 3.1 implies that

$$\mathrm{h}(a_i) \leq d\mathrm{h}(\beta) + 3d(d-1)\mathrm{h}(\alpha) + 2d(d-1)\log 2 + \log d$$

for each $i = 0, 1, \dots, d-1$. This implies the following corollary.

Corollary 3.2 *Under the same assumptions and notation as in Theorem 3.1, we have*

$$\mathrm{h}(a_i) < d\mathrm{h}(\beta) + 3d^2\mathrm{h}(\alpha) + 2d^2,$$

for $i = 0, 1, \dots, d-1$.

3.2 Proof of Theorem 3.1

In the sequel, we use the following formulas without special reference (see, *e.g.*, [20]). For any $n \in \mathbb{Z}$ and $b_1, \cdots, b_k, \gamma \in \overline{\mathbb{Q}}$, we have

$$\begin{aligned} &\mathrm{h}(b_1 + \cdots + b_k) \leq \mathrm{h}(b_1) + \cdots + \mathrm{h}(b_k) + \log k, \\ &\mathrm{h}(b_1 \cdots b_k) \leq \mathrm{h}(b_1) + \cdots + \mathrm{h}(b_k), \\ &\mathrm{h}(\gamma^n) = |n|\mathrm{h}(\gamma), \\ &\mathrm{h}(\zeta) = 0 \quad \text{for any root of unity } \zeta \in \overline{\mathbb{Q}}. \end{aligned}$$

We now assume that $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d$ are the conjugates of α over the field K. Put

$$\beta_i = \sum_{j=0}^{d-1} a_j\alpha_i^j, \qquad \text{for } i = 1, \dots, d.$$

So, $\mathrm{h}(\alpha_i) = \mathrm{h}(\alpha)$ and $\mathrm{h}(\beta_i) = \mathrm{h}(\beta)$ for $1 \leq i \leq d$.

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

To solve the above system of d linear equations in d unknowns $a_0, \dots, a_{d-1}$, we denote the appearing Vandermonde matrix by $V = (\alpha_i^{j-1})_{1\le i,j\le d}$. By [6, Formula (6)], the inverse of V is given by

$$V^{-1} = \left(\frac{(-1)^{i+j}\sigma_{d-j}(\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_d)}{\prod_{m=1}^{i-1}(\alpha_i - \alpha_m)\prod_{k=i+1}^{d}(\alpha_k - \alpha_i)} \right)^T_{1\le i,j\le d},$$

where T stands for the transpose, and $\sigma_k(\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_d)$ stands for the k-th symmetric function in the $d-1$ variables $\alpha_1, \dots, \alpha_d$ without α_i; for instance, in the case $i = d$, we have $\sigma_1(\alpha_1, \dots, \alpha_{d-1}) = \alpha_1 + \cdots + \alpha_{d-1}$ and $\sigma_{d-1}(\alpha_1, \dots, \alpha_{d-1}) = \alpha_1 \cdots \alpha_{d-1}$.

Hence,

$$(3.1) \qquad a_{j-1} = \sum_{i=1}^{d} \beta_i \frac{(-1)^{i+j}\sigma_{d-j}(\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_d)}{\prod_{m=1}^{i-1}(\alpha_i - \alpha_m)\prod_{k=i+1}^{d}(\alpha_k - \alpha_i)}.$$

Since $\sigma_{d-j}(\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_d)$ is a polynomial with coefficients 1 in $d-1$ variables $\alpha_1, \dots, \alpha_d$ (without α_i) of degree $d-j$, length $\binom{d-1}{d-j}$, and degree 1 in each variable α_k, $k \ne i$, by Lemma 2.5, we find that

$$\mathrm{h}\big(\sigma_{d-j}(\alpha_1, \dots, \widehat{\alpha_i}, \dots, \alpha_d)\big) \le \log\binom{d-1}{d-j} + \sum_{k\ne i}\mathrm{h}(\alpha_k) = \log\binom{d-1}{d-j} + (d-1)\mathrm{h}(\alpha).$$

On the other hand, in order to bound the denominator of (3.1) we observe that

$$\mathrm{h}\Big(\prod_{k\ne i}(\alpha_k - \alpha_i)\Big) \le \sum_{k\ne i}\mathrm{h}(\alpha_k - \alpha_i) \le (2d-2)\mathrm{h}(\alpha) + (d-1)\log 2,$$

since each term $\mathrm{h}(\alpha_k - \alpha_i)$ does not exceed $2\mathrm{h}(\alpha) + \log 2$.

Thus, the absolute logarithmic height of each of the d summands in (3.1) is bounded from above by

$$\mathrm{h}(\beta) + (3d-3)\mathrm{h}(\alpha) + \log\binom{d-1}{d-j} + (d-1)\log 2.$$

Hence, we conclude that

$$\mathrm{h}(a_{j-1}) \le d\Big(\mathrm{h}(\beta) + (3d-3)\mathrm{h}(\alpha) + \log\binom{d-1}{d-j} + (d-1)\log 2\Big) + \log d$$

for $j = 1, \dots, d$. By replacing $j-1$ by i and observing that

$$\binom{d-1}{d-j} = \binom{d-1}{d-i-1} = \binom{d-1}{i},$$

we see that this is exactly the required inequality of Theorem 3.1.

4 Simple Roots of Polynomials Modulo a Prime

4.1 Background and Main Results

In this section, given an irreducible polynomial $f \in \mathbb{Z}[X]$, we derive an upper bound for the smallest prime p such that f has a simple root modulo p.

First of all, we mention a sharp upper bound of Bellaïche [1] under the assumption that both the Generalized Riemann Hypothesis and the Artin Conjecture are true for the Artin L-functions associated with the irreducible representations of G, where

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

G is the Galois group of the splitting field of f over $\mathbb{Q}$. Namely, under the above assumptions, by Bellaïche [1, Théorème 16], if M is the product of all the distinct prime divisors of the discriminant of a monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degree $d \geq 1$, then

- there exists a prime $p = O(d^2(\log M + d\log d)^2)$ such that $p \nmid M$ and f has at least one root modulo p;
- there exists a prime $p = O(d^4(\log M + d\log d)^2)$ such that $p \nmid M$ and f has at least two roots modulo p.

Here, we give unconditional upper bounds of such smallest prime p for any irreducible polynomial $f \in \mathbb{Z}[X]$ without assuming that f is monic. In fact, for our purpose we need a slightly more general result where p also avoids divisors of a given integer Q.

Assume first that the polynomial f that we consider is of degree 1. Then we can take the smallest prime p that is coprime to the leading coefficient of f. So in the sequel, we suppose that the degree of f is greater than or equal to 2.

We first give a generic approach on how to find such a prime p, which yields a rather simple upper bound for p.

Theorem 4.1 *Given an irreducible polynomial $f = a_dX^d + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ of degree $d \geq 2$ and of height H, there exists a prime number*

$$p \leq \begin{cases} H, & \text{if } \gcd(a_0, M) = 1 \text{ and } |a_0| > 1,\\ 2H(dM)^d, & \text{if } |a_0| = 1,\\ 2H(dHM)^d, & \text{if } \gcd(a_0, M) > 1,\end{cases}$$

where M is the product of all the distinct prime divisors of the discriminant of f such that f has a simple root modulo p.

We now present an upper bound for such a prime p that behaves much better than that of Theorem 4.1 with respect to H (however, in some cases Theorem 4.1 is still stronger). In fact, we present it in a slightly more general form.

Theorem 4.2 *Given an irreducible polynomial $f \in \mathbb{Z}[X]$ of height H and of degree $d \geq 2$, and an integer $Q \geq 3$, there exists a prime number p satisfying*

$$p \leq C^d H(d\log Q\log^+ H)^d + H(\log Q)^{cd^2},$$

where c and C some absolute constants such that f has a root modulo p and $p \nmid Q$.

We denote the discriminant of f by Δ. Choosing $Q = 3|\Delta|$ we derive the following corollary.

Corollary 4.3 *Given an irreducible polynomial $f \in \mathbb{Z}[X]$ of height H and of degree $d \geq 2$, there exists a prime number p satisfying $p \leq H(d\log^+ H)^{O(d^2)}$, such that f has a simple root modulo p.*

Remark 4.4 Let f be the n-th cyclotomic polynomial with $n > 2$. Then it is well known that, for a prime p, f has a simple root modulo p if and only if $p \equiv 1 \pmod{n}$.

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

Linnik's theorem says that such a prime p can be chosen so that $p = O(n^L)$, where L is an absolute constant. A recent result of Xylouris [23] says that we can choose $L = 5.18$.

4.2 Products of Polynomial Values

First, we give a lower bound on the product of polynomial values that is necessary for our argument and can be of independent interest.

Lemma 4.5 *Let $f \in \mathbb{C}[x]$ be a polynomial of degree $d \geq 1$, and assume that the absolute value of the leading coefficient of f is not less than 1. Then for each integer $L \geq 51(2d+1)$, we have*

$$\prod_{j=1}^{L} \max\{1, |f(j)|\} \geq (L/5)^{dL/18}.$$

Proof Call a point $j \in S = \{1, 2, \dots, L\}$ *good* if the distance from j to the nearest root of f is at least 1. Then $|f(j)| \geq 1$. Since each open disc of radius 1 and center at a root of f contains at most two points of the set S, there are at least $L - 2d$ good points in S.

Consider four open discs D_1, D_2, D_3, D_4 of radius $L/6$ each, with centers at $L/10$, $11L/30$, $19L/30$, $9L/10$, respectively, and put $D_5 := \mathbb{C} \setminus \bigcup_{j=1}^{4} D_j$. It is easy to see that the distance from each point of the set S to D_5 is at least

$$\min\Big\{ L/6 - L/10, \sqrt{(L/6)^2 - (2L/15)^2} \Big\} = \min\{L/15, L/10\} = L/15.$$

Now, if at least $d/10$ roots of f lie in D_5, we obtain $|f(j)| \geq (L/15)^{d/10}$ for each good $j \in S$. Thus, as $L \geq 100d$, we deduce

$$\prod_{j=1}^{L} \max\{1, |f(j)|\} \geq \prod_{j-\text{good}} |f(j)| \geq (L/15)^{(L-2d)d/10} > (L/15)^{2dL/21} > (L/5)^{dL/17},$$

which is stronger than required.

Alternatively, when D_5 contains less than $d/10$ roots of f, the union $\bigcup_{j=1}^{4} D_j$ must contain at least $0.9d$ roots of f. Thus, some D_i, where $i \in \{1, 2, 3, 4\}$, contains at least $0.225d$ roots of f. Now, we put $k = 1$ if $i = 3$ or $i = 4$, and $k = 4$ if $i = 1$ or $i = 2$. The set D_k contains at least $4L/15 - 2d - 1 \geq 0.247L$ good points of S. (Here, we use the bound $L \geq 51(2d+1)$.) The distance between any two points of D_k and D_i is at least $19L/30 - L/6 - (L/10 + L/6) = L/5$. Consequently, the distance from each good point in D_k to D_i is at least $L/5$. Thus,

$$\prod_{j=1}^{L} \max\{1, |f(j)|\} \geq \prod_{j-\text{good in } D_k} |f(j)| \geq (L/5)^{0.247L\cdot 0.225d} > (L/5)^{dL/18}.$$

This completes the proof. ∎

Note that the lower bound of Lemma 4.5 is sharp up to the constants. For instance, for $f(x) = x^d$, we have

$$\prod_{j=1}^{L} \max\{1, |f(j)|\} = L!^d \leq L^{dL}.$$

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

4.3 Polynomial Congruences

For a polynomial $f \in \mathbb{Z}[X]$ of degree $d \geq 1$ and two positive integers L and q, we define

$$N(L,q) = \big|\{1 \leq j \leq L : f(j) \equiv 0 \pmod q\}\big| \quad \text{and} \quad N(q) = N(q,q).$$

Recall that the *content* of a polynomial f is defined as the greatest common divisor of the coefficients of f. We also need the following three bounds on $N(L,q)$ when $q = \ell^k$ is a prime power.

Lemma 4.6 *Given a positive integer k and a prime number ℓ, suppose that the content of f is coprime to ℓ, and that f has m distinct zeros over $\mathbb{C}$. Then we have $N(\ell^k) \leq m\ell^{k-1}$.*

Lemma 4.7 *Given a positive integer k and a prime number ℓ, suppose that the content of f is coprime to ℓ. Then we have $N(\ell^k) \leq 2\ell^{k(1-1/d)}$.*

Lemma 4.8 *Given positive integers L, k, and a prime number ℓ, we have*

$$\Big|N(L,\ell^k) - \frac{L}{\ell^k}N(\ell^k)\Big| < d.$$

Lemma 4.6 is well known and also trivial; Lemmas 4.7 and 4.8 follow directly from [7, Lemma 2] and [8, Theorem 1], respectively.

4.4 Prime Divisors of Polynomial Products

The following uniform lower bound on the number of prime divisor is one of our main technical tools but may also be of independent interest.

As usual, let $\omega(k)$ denote the number of distinct prime divisors of an integer $k \geq 1$.

Lemma 4.9 *There are absolute constants $c_1, c_2 > 0$ such that for any polynomial $f(X) \in \mathbb{Z}[X]$ of degree $d \geq 1$ and of height H, for each integer $L \geq 2d+1$, for the product*

$$W(L) = \prod_{j=1}^{L} \max\{1, |f(j)|\},$$

we have

$$\omega\big(W(L)\big) \geq \min\Big\{\frac{c_1 L}{\log^+ H}, L^{c_2/d}\Big\}.$$

Proof Let $t = \omega(W(L))$ be the number of distinct prime divisors of $W(L)$. Since $L \geq 2d+1$, we obviously have $W(L) \geq 2$, so we also have $t \geq 1$. Thus, adjusting the constant c_1 we can assume that $L \geq 51(2d+1)$.

For a prime ℓ, we define $r_\ell(L)$ by $\ell^{r_\ell(L)} \| W(L)$. Then we have

$$r_\ell(L) = \sum_{k=1}^{K_\ell(L)} N(L,\ell^k),$$

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

where $N(L,\ell^k)$ is as in Section 4.3 and

$$K_\ell(L)=\max\big\{r:\exists 1\le j\le L,\ \ell^r\mid f(j), f(j)\ne 0\big\}.$$

Clearly, $|f(j)|\le 2HL^d$ for $1\le j\le L$. Therefore,

$$K_\ell(L)\le\log(2HL^d)/\log\ell. \tag{4.1}$$

We use Lemma 4.6 for $k\le d$ and Lemma 4.7 for $k>d$. Furthermore, from Lemma 4.8, we find that

$$\begin{aligned} r_\ell(L) &\le L\sum_{k=1}^{K_\ell(L)}\frac{N(\ell^k)}{\ell^k}+dK_\ell(L)\le L\sum_{k=1}^{d}\frac{d}{\ell}+L\sum_{k=d+1}^{\infty}2\ell^{-k/d}+dK_\ell(L)\\ &=d^2L\ell^{-1}+\frac{2L\ell^{-1}}{\ell^{1/d}-1}+dK_\ell(L). \end{aligned}$$

Notice that since $\log x\le x-1$ for $x>0$, we have

$$\frac{1}{\ell^{1/d}-1}\le\frac{d}{\log\ell}.$$

Then

$$r_\ell(L)\le d^2L\ell^{-1}+2dL\ell^{-1}(\log\ell)^{-1}+dK_\ell(L)<(d+3)dL\ell^{-1}+dK_\ell(L).$$

Therefore, recalling (4.1), we obtain

$$\ell^{r_\ell(L)}\le(2HL^d)^d\exp\Big((d+3)dL\frac{\log\ell}{\ell}\Big).$$

Let $\mathcal{L}$ be the set of distinct prime divisors of $W(L)$. Then we have

$$|W(L)|\le(2HL^d)^{dt}\exp\Big((d+3)dL\sum_{\ell\in\mathcal{L}}\frac{\log\ell}{\ell}\Big).$$

Notice that

$$\sum_{\ell\in\mathcal{L}}\frac{\log\ell}{\ell}=O(\log t),$$

because it is bounded by the sum over the first t primes. Hence,

$$|W(L)|\le(2HL^d)^{dt}\exp\big(O(d^2L\log t)\big). \tag{4.2}$$

Denoting by T_1 and T_2 the two terms in the product on the right-hand side of (4.2) (so that $|W(L)|\le T_1T_2$), we see that at least one of the inequalities $|W(L)|\le T_1^2$ or $|W(L)|\le T_2^2$ holds. More precisely, we have

$$|W(L)|\le(2HL^d)^{2dt} \tag{4.3}$$

or

$$|W(L)|=\exp\big(O(d^2L\log t)\big). \tag{4.4}$$

On the other hand, by Lemma 4.5, if $L\ge 51(2d+1)$, we have

$$|W(L)|\ge(L/5)^{dL/18}. \tag{4.5}$$

If (4.3) holds, then comparing (4.3) and (4.5), we find that

$$t\ge\frac{c_1L}{d\log^+H},$$

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

where c_1 is some absolute constant.

Alternatively, if (4.4) holds, then applying the same argument, but using (4.4) and (4.5), we obtain $t \geq L^{c_2/d}$, where c_2 is an absolute constant. This completes the proof. ■

4.5 Proofs

Proof of Theorem 4.1 If $\gcd(a_0, M) = 1$ and $|a_0| > 1$, then we pick a prime divisor p of a_0. Then 0 a simple root of f modulo p, and, clearly, $p \leq H$.

Suppose $|a_0| = 1$. Compute $f(\pm iM)$, $0 \leq i \leq d$. Then there exists at least one i_0 such that $|f(i_0 M)| \neq 1$ or $|f(-i_0 M)| \neq 1$. Assume that $|f(i_0 M)| \neq 1$ without loss of generality. Pick a prime divisor p of $f(i_0 M)$. Since $p \nmid M$, $i_0 M$ is exactly a simple root of f modulo p. So, $p \leq 2H(dM)^d$.

Finally, suppose that $m = \gcd(a_0, M) > 1$. Compute $f(\pm i a_0 M)$, $0 \leq i \leq d$. Then, there exists at least one i_0 such that $|f(i_0 a_0 M)| \neq |a_0|$ or $|f(-i_0 a_0 M)| \neq |a_0|$. Assume that $|f(i_0 a_0 M)| \neq |a_0|$ without loss of generality. Pick a prime divisor p of $f(i_0 a_0 M)/a_0$. Since $p \nmid M$, $i_0 a_0 M$ is exactly a simple root of f modulo p. So, $p \leq 2H(dHM)^d$. ■

Proof of Theorem 4.2 First, we note that for the irreducible polynomial f we consider, since the units of $\mathbb{Z}[X]$ are exactly ± 1, the content of f is 1.

Let $s = \omega(Q)$. Clearly,

$$s \leq \frac{\log Q}{\log 2} < 2 \log Q.$$

Let $W(L)$ be the product of Lemma 4.9 and let $t = \omega(W(L))$ be the number of distinct prime divisors of $W(L)$.

Our goal is to show that for some sufficiently small L we have $s < t$, which in turn immediately yields the bound

$$p \leq \max\{|f(j)| : j = 1, \ldots, L\} \tag{4.6}$$

on the desired prime p.

By Lemma 4.9 we either have

$$t \geq \frac{c_1 L}{d \log^+ H}, \tag{4.7}$$

or

$$t \geq L^{c_2/d}, \tag{4.8}$$

If (4.7) holds, then it is sufficient to require that

$$L \geq c_3 d \log Q \log^+ H \tag{4.9}$$

for some absolute constant $c_3 > 0$.

If (4.8) holds, then it suffices to require that

$$L \geq (\log Q)^{c_4 d} \tag{4.10}$$

for some absolute constant c_4.

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

Finally, comparing (4.9) with (4.10), we choose

$$L = \left\lceil C_0 d \log Q \log^+ H + (\log Q)^{c_0 d} \right\rceil,$$

where c_0 and C_0 are some sufficiently large absolute constants. Now, from (4.6) it is easy to see that we can choose a prime

$$p \le 2HL^d \le C^d H(d \log Q \log^+ H)^d + H(\log Q)^{cd^2}$$

for some absolute constants c and C such that f has a root modulo p and $p \nmid Q$. ∎

Proof of Corollary 4.3 We recall that by [11, Theorem 1] and (2.1), the discriminant Δ of f satisfies

$$|\Delta| < d^{2d} H^{2d-2}. \tag{4.11}$$

The required result now follows from Theorem 4.2. ∎

5 Explicit Form of Cassels' p-adic Embedding Theorem

5.1 Arbitrary Number Fields

Let K be a number field of degree $d \ge 2$, and let $\beta_1, \dots, \beta_n$ be some fixed non-zero elements of K. By Theorem 1.1, there exist infinitely many primes p such that there is an embedding

$$\sigma\colon K \hookrightarrow \mathbb{Q}_p \tag{5.1}$$

for which $|\sigma(\beta_i)|_p = 1$, for $1 \le i \le n$. In order to prove Theorem 1.2, we derive an upper bound for such a prime p.

First, we assume that $K = \mathbb{Q}(\alpha)$ and that the minimal polynomial of α over $\mathbb{Z}$ is f. Put

$$S = \{\beta_1, \dots, \beta_n, \beta_{n+1}, \dots, \beta_{2n}\},$$

where $\beta_{n+i} = \beta_i^{-1}$ for $1 \le i \le n$. So, in order to ensure that $|\sigma(\beta_i)|_p = 1$ for $1 \le i \le n$, we only need to ensure that $|\sigma(\beta_i)|_p \le 1$ for $1 \le i \le 2n$.

Note that every β_i, $1 \le i \le 2n$, can be expressed uniquely as

$$\beta_i = \frac{1}{b_i}(a_{i,0} + a_{i,1}\alpha + \cdots + a_{i,d-1}\alpha^{d-1}),$$

where $b_i, a_{i,0}, \dots, a_{i,d-1} \in \mathbb{Z}$, $b_i \ge 1$, and $\gcd(a_{i,0}, \dots, a_{i,d-1}) = 1$. Moreover, for $1 \le i \le 2n$, applying Corollary 3.2, we find that

$$\log b_i \le \max_{0 \le j \le d-1} \mathrm{h}(a_{i,j}/b_i) < d\mathrm{h}(\beta_i) + 3d^2\mathrm{h}(\alpha) + 2d^2. \tag{5.2}$$

We claim that a prime p satisfies (5.1) if it satisfies the following three conditions:

(a) $f(a) \equiv 0 \pmod p$ for some $a \in \mathbb{Z}$,
(b) $\Delta \not\equiv 0 \pmod p$, where Δ is the discriminant of f,
(c) $b_i \not\equiv 0 \pmod p$, for $1 \le i \le 2n$.

Indeed, if f satisfies Conditions (a) and (b), then, by Hensel's lemma, there exists an element $\eta \in \mathbb{Z}_p$ such that $f(\eta) = 0$, where $\mathbb{Z}_p$ denotes the set of p-adic integers. Then, we define an embedding $\sigma\colon K \to \mathbb{Q}_p$, by setting $\sigma(\alpha) = \eta$. Under Condition (c), we can see that $|\sigma(\beta_i)|_p \le 1$ for $1 \le i \le 2n$.

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

Therefore, to get an upper bound for such smallest prime p satisfying (5.1), we can use Theorem 4.2 directly with $Q = 3|\Delta|b_1 \cdots b_{2n}$ by applying (4.11) and (5.2). It follows that we can pick a prime p satisfying (5.1) and such that

$$p \le H\Big(dn\mathrm{h}(\alpha) + d\sum_{i=1}^{n} \mathrm{h}(\beta_i) + d\log^{+} H + dn\Big)^{O(d^2)},$$

where $H = H(f)$ is the height of f.

In addition, by (2.1), we find that $H \le 2^d \exp(d\mathrm{h}(\alpha))$. So, we obtain

$$p \le H\Big(dn\mathrm{h}(\alpha) + d\sum_{i=1}^{n} \mathrm{h}(\beta_i) + dn\Big)^{O(d^2)}$$

and

$$p \le \exp(d\mathrm{h}(\alpha))\Big(dn\mathrm{h}(\alpha) + d\sum_{i=1}^{n} \mathrm{h}(\beta_i) + dn\Big)^{O(d^2)}. \tag{5.3}$$

Proof of Theorem 1.2 Since K is generated by $\alpha_1, \dots, \alpha_m \in K \setminus \mathbb{Q}$ over $\mathbb{Q}$, by Theorem 2.1, there exists an algebraic number α such that $K = \mathbb{Q}(\alpha)$ and

$$\mathrm{h}(\alpha) \le \log(dm) + \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_m).$$

Thus,

$$\exp(d\mathrm{h}(\alpha)) \le (dm)^d \exp\Big(d\sum_{i=1}^{m} \mathrm{h}(\alpha_i)\Big)$$

and

$$\begin{aligned} dn\mathrm{h}(\alpha) + d\sum_{i=1}^{n} \mathrm{h}(\beta_i) + dn &\le d\Big(n\sum_{i=1}^{m} \mathrm{h}(\alpha_i) + \sum_{i=1}^{n} \mathrm{h}(\beta_i) + n\log(dm) + n\Big) \\ &= O\Big(\Big(n\sum_{i=1}^{m} \mathrm{h}(\alpha_i) + \sum_{i=1}^{n} \mathrm{h}(\beta_i) + n\log^{+} m\Big) d\log d\Big). \end{aligned}$$

Combining these two inequalities with (5.3), we see that p satisfies the inequality

$$p \le m^d \exp\Big(d\sum_{i=1}^{m} \mathrm{h}(\alpha_i)\Big)\Big(n\sum_{i=1}^{m} \mathrm{h}(\alpha_i) + \sum_{i=1}^{n} \mathrm{h}(\beta_i) + n\log^{+} m\Big)^{O(d^2)} d^{O(d^2)},$$

which concludes the proof. ∎

Proof of Corollary 1.3 It is easy to see that the result follows directly from Theorem 1.2. ∎

Proof of Corollary 1.4 We only need to notice that for the fixed algebraic integers (resp., units) $\beta_1, \dots, \beta_n \in \mathbb{Z}[\alpha]$, $b_i = 1$ for $1 \le i \le n$ (resp., $1 \le i \le 2n$). Then the result follows directly from Corollary 4.3 and (2.1). ∎

Proof of Corollary 1.5 Since K has at least one real embedding, by [19, Theorem 1.2], there exists an element α of K such that $K = \mathbb{Q}(\alpha)$ and

$$\mathrm{h}(\alpha) \le \frac{\log|D_K|}{2d}.$$

Notice that $|D_K| \ge 7.25^d$ when $d \ge 16$; see [13, Section 2]. Then the desired result follows from (5.3). ∎

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

5.2 Cyclotomic Fields

In this section, we consider the special case when K is the m-th cyclotomic field with $m > 2$, namely, $K = \mathbb{Q}(\zeta_m)$, where ζ_m is an m-th primitive root of unity. Fix some non-zero elements $\beta_1, \dots, \beta_n$ of K. We want to get an upper bound for the smallest prime p such that there is an embedding

$$\sigma\colon K \hookrightarrow \mathbb{Q}_p \tag{5.4}$$

for which $|\sigma(\beta_i)|_p = 1$, for $1 \le i \le n$.

In order to obtain a better bound, we need to refine (4.7) and (4.8) in this special case. Here, we use the notation in Section 4.5 without special indication. We also note that in this case f is the m-th cyclotomic polynomial, and the degree of K (or f) is $d = \phi(m)$.

Proof of Theorem 1.6 Recall that, for a prime ℓ, we have $\ell^e \| m$. In particular, $e = 0$ when $\ell \nmid m$. By the basic theory of cyclotomic fields (for example, see [21, Chapter 2]), f has a root modulo ℓ if and only if f can be factored completely modulo ℓ, and if and only if $\ell \equiv 1 \pmod{m/\ell^e}$. In particular, if $\ell \equiv 1 \pmod{m/\ell^e}$, then f has $\phi(m/\ell^e)$ distinct roots modulo ℓ. Moreover, if $\ell \mid m$, then $\ell \equiv 1 \pmod{m/\ell^e}$ is possible only when $\ell = P(m)$, where, as before, $P(m)$ denotes the largest prime divisor of m.

Combining the above considerations with [18, Corollary 2], for a prime $\ell \nmid m$ and any integer $k \ge 1$, we have

$$N(\ell^k) \le \begin{cases} d, & \text{if } \ell \equiv 1 \pmod{m}, \\ 0, & \text{otherwise.} \end{cases}$$

So, for a prime $\ell \nmid m$, we obtain

$$r_\ell(L) \le L \sum_{k=1}^{\infty} \frac{d}{\ell^k} + dK_\ell(L) \le 2dL\ell^{-1} + dK_\ell(L). \tag{5.5}$$

Next, for any prime number ℓ and integer $k \ge 1$, it is easy to see that $N(\ell^k) \le \ell N(\ell^{k-1}) \le \cdots \le \ell^{k-1}N(\ell)$. Then, for a prime $\ell \mid m$ and $\ell^e \| m$, we find that

$$N(\ell) = \begin{cases} \phi(m/\ell^e), & \text{if } \ell = P(m) \text{ and } \ell \equiv 1 \pmod{m/\ell^e}, \\ 0, & \text{otherwise;} \end{cases}$$

and for $k \ge 2$,

$$N(\ell^k) \le \begin{cases} \phi(m/\ell^e)\ell^{k-1}, & \text{if } \ell = P(m) \text{ and } \ell \equiv 1 \pmod{m/\ell^e}, \\ 0, & \text{otherwise.} \end{cases}$$

Thus, for a prime $\ell \mid m$ and $\ell^e \| m$, applying the same arguments as those in Section 4.5, we derive that

$$r_\ell(L) \le \begin{cases} (\phi(m/\ell^e) + 3)dL\ell^{-1} + dK_\ell(L), & \text{if } \ell = P(m) \text{ and } \ell \equiv 1 \pmod{m/\ell^e}, \\ dK_\ell(L), & \text{otherwise.} \end{cases}$$

Therefore, comparing this inequality with (5.5), for any prime ℓ, we deduce

$$r_\ell(L) \le 4dL\delta(m)\ell^{-1} + dK_\ell(L),$$

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

where $\delta(m)$ has been defined in Section 1.

Then applying the same arguments as Section 4.5, for $L \ge 51(2d+1)$, we can deduce the following analogue of (4.7) and (4.8):

$$t \ge \frac{c_1 L}{d \log^+ H} \quad \text{or} \quad t \ge L^{c_2/\delta(m)},$$

where c_1 and c_2 are two absolute constants, and $H = H(f)$. So, for any integer $Q \ge 3$, we can choose a prime p satisfying

$$p \le C^d H(d \log Q \log^+ H)^d + H(\log Q)^{cd\delta(m)}$$

for some absolute constants c and C, and such that f has a root modulo p and $p \nmid Q$.

Finally, applying the same arguments as Section 5.1 and noticing that $\mathrm{h}(\zeta_m) = 0$, we get the following upper bound for the smallest such prime number p satisfying (5.4):

$$p \le \Big(d \sum_{i=1}^{n} \mathrm{h}(\beta_i) + dn \Big)^{O(d\delta(m))},$$

where $d = \phi(m)$. ∎

6 Comments

It is certainly interesting to understand how tight our bounds are. Denoting by p_k the k-th prime number and defining

$$\beta_i = \prod_{r=0}^{R-1} p_{nr+i}, \qquad i = 1, \dots, n,$$

for some sufficiently large integer parameter R, we see from the prime number theorem that

$$\prod_{i=1}^{n} \beta_i = \exp\big((1 + o(1)) nR \log(nR) \big).$$

On the other hand, the smallest prime p with $|\sigma(\beta_i)|_p = 1$, for $1 \le i \le n$, obviously satisfies

$$p > p_{nR} = \big(1 + o(1)\big) nR \log(nR) = \big(1 + o(1)\big) \sum_{i=1}^{n} \mathrm{h}(\beta_i).$$

Here is a less obvious example that illustrates the sharpness of our results in Section 2 for $d = 2$. Although in our application we do not need so strong result, by a recent groundbreaking results of Maynard [12] and Zhang [24], there exists a positive integer t such that $k + t$ and $k - t$ are both prime for infinitely many positive integers k. Take k large enough and consider the following quadratic polynomial $f_k(x) = x^2 - 2kx + t^2$ with height $2k$. Its splitting field is $K = \mathbb{Q}(\sqrt{(k+t)(k-t)})$, so each α satisfying $K = \mathbb{Q}(\alpha)$ is of the form

$$\alpha = a + b\beta \quad \text{with} \quad \beta = \sqrt{(k+t)(k-t)}$$

and rational a and $b \ne 0$. We claim that $H(\alpha) > n/3$ for all such α. To prove this, assume that $a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$, where $a_2 > 0$, is the minimal polynomial of

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press

$\alpha = a + b\beta$ and write $b = b_0/b_1$ with coprime $b_0 \in \mathbb{Z} \smallsetminus \{0\}$ and $b_1 \in \mathbb{N}$. Note that the discriminant of $a_2x^2 + a_1x + a_0$ is

$$a_1^2 - 4a_0a_2 = a_2^2(a + b\beta - a + b\beta)^2 = a_2^2(2b\beta)^2 = \frac{4a_2^2b_0^2(k+t)(k-t)}{b_1^2}.$$

In particular, this yields that $b_1^2 \mid 4a_2^2(k+t)(k-t)$.

Now, if $k+t$ or $k-t$ is a prime divisor of b_1, then this divisor also divides a_2. Thus, $H(\alpha) \geq |a_2| \geq k - t > k/2$, which is stronger than claimed. If, otherwise, neither $k+t$ nor $k-t$ divides b_1, then $4a_2^2/b_1^2$ is an integer, so $b_1^2 \leq 4a_2^2b_0^2$. It follows that

$$\begin{aligned}(k+t)(k-t) &= \frac{b_1^2}{4a_2^2b_0^2}(a_1^2 - 4a_0a_2) \leq a_1^2 + 4|a_0|a_2\\ &\leq 5\max\{|a_0|,|a_1|,|a_2|\}^2 = 5H(\alpha)^2.\end{aligned}$$

This implies the inequality $H(\alpha) > k/3$, as claimed (provided that k is large enough). Hence, our example shows that the exponent $(d-1)D/d$ in Corollary 2.3 is sharp for $d = 2$ (in this case we automatically have $D = 2$).

References

[1] J. Bellaïche, *Théorème de Chebotarev et complexité de Littlewood*. arxiv:1308.1022.

[2] J. W. Brawley and S. Gao, *On density of primitive elements for field extensions.* http://www.math.clemson.edu/~sgao/papers/prim-ele.pdf.

[3] R. D. Carmichael and T. E. Mason, *Note on the roots of algebraic equations.* Bull. Amer. Math. Soc. **21**(1914), no. 1, 14–22. http://dx.doi.org/10.1090/S0002-9904-1914-02563-7

[4] J. W. S. Cassels, *An embedding theorem for fields.* Bull. Austral. Math. Soc. **14**(1976), no. 2, 193–198. http://dx.doi.org/10.1017/S000497270002503X

[5] G. Everest, A. J. van der Poorten, I. E. Shparlinski, and T. Ward, *Recurrence sequences*. Mathematical Surveys and Monographs, 104, American Mathematical Society, Providence, RI, 2003.

[6] A. Klinger, *The Vandermonde matrix*. Amer. Math. Monthly, **74**(1967), 571–574. http://dx.doi.org/10.2307/2314898

[7] S. V. Konyagin, *On the number of solutions of an nth degree congruence with one unknown*. Matem. Sb. (N.S.) **109(151)**(1979), no. 2, 171–187; English version: Math. USSR-Sb. **37**(1980), 151–166.

[8] S. V. Konyagin and T. Steger, *On polynomial congruences*. Math. Notes **55**(1994), no. 5–6, 596–600.

[9] E. Landau, *Über eine Aufgabe der Funktionentheorie.* Tohoku Math. J. **5**(1914), 97–116.

[10] J. H. Loxton and A. J. van der Poorten, *On the growth of recurrence sequences*. Math. Proc. Cambridge Philos. Soc. **81**(1977), 369–376. http://dx.doi.org/10.1017/S0305004100053445

[11] K. Mahler, *An inequality for the discriminant of a polynomial.* Michigan Math. J. **11**(1964), 257–262. http://dx.doi.org/10.1307/mmj/1028999140

[12] J. Maynard, *Small gaps between primes*. Annals of Math. **181**(2015), no. 1, 383–413. http://dx.doi.org/10.4007/annals.2015.181.1.7

[13] A. M. Odlyzko, *Some analytic estimates of class numbers and discriminants.* Invent. Math. **29**(1975), no. 3, 275–286. http://dx.doi.org/10.1007/BF01389854

[14] A. J. van der Poorten and H.-P. Schlickewei, *Additive relations in fields.* J. Austral. Math. Soc. **51**(1991), no. 1, 154–170. http://dx.doi.org/10.1017/S144678870003336X

[15] A. J. van der Poorten and I. E. Shparlinski, *On the number of zeros of exponential polynomials and related questions*. Bull. Austral. Math. Soc. **46**(1992), no. 3, 401–412. http://dx.doi.org/10.1017/S0004972700012065

[16] ———, *On sequences of polynomials defined by certain recurrence relations*. Acta Sci. Math. (Szeged) **61**(1995), no. 1–4, 77–103.

[17] W. Specht, *Abschätzungen der Wurzeln algebraischer Gleichungen*. Math. Z. **52**(1949), 310–321. http://dx.doi.org/10.1007/BF02230697

[18] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*. J. Amer. Math. Soc. **4**(1991), no. 4, 793–835. http://dx.doi.org/10.1090/S0894-0347-1991-1119199-X

[19] J. D. Vaaler and M. Widmer, *A note on small generators of number fields*. In: Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics, 587, American Mathematical Society, Providence, RI, 2013.

[20] M. Waldschmidt, *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables.* Grundlehren der Mathematischen Wissenschaften, 326, Springer, Berlin, 2000.

[21] L. C. Washington, *Introduction to cyclotomic fields*. Graduate Texts in Mathematics, 83, Springer, New York, 1982.

[22] M. Widmer, *Counting primitive points of bounded height.* Trans. Amer. Math. Soc. **362**(2010), no. 9, 4793–4829. http://dx.doi.org/10.1090/S0002-9947-10-05173-1

[23] T. Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*. Acta Arith. **150**(2011), no. 1, 65–91. http://dx.doi.org/10.4064/aa150-1-4

[24] Y. Zhang, *Bounded gaps between primes*. Ann. of Math. **179**(2014), no. 3, 1121–1174. http://dx.doi.org/10.4007/annals.2014.179.3.7

Department of Mathematics and Informatics, Vilnius University, LT-03225 Vilnius, Lithuania
e-mail: arturas.dubickas@mif.vu.lt

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia
e-mail: shamin2010@gmail.com igor.shparlinski@unsw.edu.au

https://doi.org/10.4153/CJM-2015-021-2 Published online by Cambridge University Press