Acta Math., 211 (2013), 291–314
DOI: 10.1007/s11511-013-0105-y

On divisors of Lucas and Lehmer numbers

by

Cameron L. Stewart

University of Waterloo
Waterloo, ON, Canada

1. Introduction

Let u_n be the nth term of a Lucas sequence or a Lehmer sequence. In this article we shall establish an estimate from below for the greatest prime factor of u_n which is of the form $n\exp(\log n/104\log\log n)$. In so doing we are able to resolve a question of Schinzel from 1962 and a conjecture of Erdős from 1965. In addition we are able to give the first general improvement on results of Bang from 1886 and Carmichael from 1912.

Let α and β be complex numbers such that $\alpha+\beta$ and $\alpha\beta$ are non-zero coprime integers and α/β is not a root of unity. Put

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}\quad \text{for } n\geqslant 0.$$

The integers u_n are known as *Lucas numbers* and their divisibility properties have been studied by Euler, Lagrange, Gauss, Dirichlet and others (see [11, Chapter XVII]). In 1876 Lucas [24] announced several new results concerning Lucas sequences $\{u_n\}_{n=0}^{\infty}$ and in a substantial paper in 1878 [25] he gave a systematic treatment of the divisibility properties of Lucas numbers and indicated some of the contexts in which they appeared. Much later Matijasevich [26] appealed to these properties in his solution of Hilbert's 10th problem.

For any integer m let $P(m)$ denote the greatest prime factor of m with the convention that $P(m)=1$ when m is 1, 0 or -1. In 1912 Carmichael [8] proved that if α and β are real and $n>12$ then

$$P(u_n)\geqslant n-1. \tag{1.1}$$

Research supported in part by the Canada Research Chairs Program and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

Results of this character had been established earlier for integers of the form a^n-b^n, where a and b are integers with $a>b>0$. Indeed Zsigmondy [49] in 1892 and Birkhoff and Vandiver [6] in 1904 proved that, for $n>2$,

$$P(a^n-b^n)\geqslant n+1, \tag{1.2}$$

while in the special case that $b=1$ the result is due to Bang [4] in 1886.

In 1930 Lehmer [23] showed that the divisibility properties of Lucas numbers hold in a more general setting. Suppose that $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime non-zero integers with α/β not a root of unity and, for $n>0$, put

$$\tilde{u}_n=\begin{cases}\dfrac{\alpha^n-\beta^n}{\alpha-\beta} & \text{for } n \text{ odd,}\\ \dfrac{\alpha^n-\beta^n}{\alpha^2-\beta^2} & \text{for } n \text{ even.}\end{cases}$$

Integers of the above form have come to be known as *Lehmer numbers*. Observe that Lucas numbers are also Lehmer numbers up to a multiplicative factor of $\alpha+\beta$ when n is even. In 1955 Ward [45] proved that if α and β are real then, for $n>18$,

$$P(\tilde{u}_n)\geqslant n-1, \tag{1.3}$$

and four years later Durst [13] observed that (1.3) holds for $n>12$.

A prime number p is said to be a *primitive divisor* of a Lucas number u_n if p divides u_n but does not divide $(\alpha-\beta)^2u_2\ldots u_{n-1}$. Similarly p is said to be a *primitive divisor* of a Lehmer number $\tilde{u}_n$ if p divides $\tilde{u}_n$ but does not divide $(\alpha^2-\beta^2)^2\tilde{u}_3\ldots\tilde{u}_{n-1}$. For any integer $n>0$ and any pair of complex numbers α and β, we denote the *n-th cyclotomic polynomial* in α and β by $\Phi_n(\alpha,\beta)$, so

$$\Phi_n(\alpha,\beta)=\prod_{\substack{j=1\\(j,n)=1}}^{n}(\alpha-\zeta^j\beta),$$

where ζ is a primitive nth root of unity. One may check, see [38], that $\Phi_n(\alpha,\beta)$ is an integer for $n>2$ if $(\alpha+\beta)^2$ and $\alpha\beta$ are integers. Further, see [38, Lemma 6], if in addition $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime non-zero integers, α/β is not a root of unity, $n>4$ and n is not 6 or 12, then $P(n/(3,n))$ divides $\Phi_n(\alpha,\beta)$ to at most the first power and all other prime factors of $\Phi_n(\alpha,\beta)$ are congruent to 1 or -1 modulo n. The last assertion can be strengthened in the case that α and β are coprime integers to the assertion that all other prime factors of $\Phi_n(\alpha,\beta)$ are congruent to 1 modulo n. Since

$$\alpha^n-\beta^n=\prod_{d\mid n}\Phi_d(\alpha,\beta), \tag{1.4}$$

$\Phi_1(\alpha,\beta)=\alpha-\beta$ and $\Phi_2(\alpha,\beta)=\alpha+\beta$, we see that if n exceeds 2 and p is a primitive divisor of a Lucas number u_n or Lehmer number $\tilde{u}_n$, then p divides $\Phi_n(\alpha,\beta)$. Further, a primitive divisor of a Lucas number u_n or Lehmer number $\tilde{u}_n$ is not a divisor of n and so it is congruent to $\pm 1 \pmod{n}$. Estimates (1.1)–(1.3) follow as consequences of the fact that the nth term of the sequences in question possesses a primitive divisor. It was not until 1962 that this approach was extended to the case where α and β are not real by Schinzel [30]. He proved, by means of an estimate for linear forms in two logarithms of algebraic numbers due to Gel′fond [17], that there is a positive number C, which is effectively computable in terms of α and β, such that if n exceeds C then $\tilde{u}_n$ possesses a primitive divisor. In 1974 Schinzel [35] employed an estimate of Baker [2] for linear forms in the logarithms of algebraic numbers to show that C can be replaced by a positive number C_0, which does not depend on α and β, and in 1977 Stewart [39] showed that C_0 could be taken to be $e^{452}4^{67}$. This was subsequently refined by Voutier [43], [44] to 30030. In addition Stewart [39] proved that C_0 can be taken to be 6 for Lucas numbers and 12 for Lehmer numbers with finitely many exceptions and that the exceptions could be determined by solving a finite number of Thue equations. This program was successfully carried out by Bilu, Hanrot and Voutier [5], and as a consequence they were able to show that for $n>30$ the nth term of a Lucas or Lehmer sequence has a primitive divisor. Thus (1.1) and (1.3) hold for $n>30$ without the restriction that α and β be real.

In 1962 Schinzel [31] asked if there exists a pair of integers a and b with ab different from $\pm 2c^2$ and $\pm c^h$, with $h\geqslant 2$, for which $P(a^n-b^n)$ exceeds $2n$ for all sufficiently large n. In 1965 Erdős [14] conjectured that

$$\frac{P(2^n-1)}{n}\to\infty \quad \text{as } n\to\infty.$$

Thirty-five years later Murty and Wong [28] showed that Erdős' conjecture is a consequence of the abc conjecture [41]. They proved, subject to the abc conjecture, that if ε is a positive real number and a and b are integers with $a>b>0$, then

$$P(a^n-b^n)>n^{2-\varepsilon},$$

provided n is sufficiently large in terms of a, b and ε. In 2004 Murata and Pomerance [27] proved, subject to the generalized Riemann hypothesis, that

$$P(2^n-1)>\frac{n^{4/3}}{\log\log n} \tag{1.5}$$

for a set of positive integers n of asymptotic density 1.

The first unconditional refinement of (1.2) was obtained by Schinzel [31] in 1962. He proved that if a and b are coprime and ab is a square or twice a square, then

$$P(a^n-b^n)\geqslant 2n+1,$$

provided that one excludes the cases $n=4,6,12$ when $a=2$ and $b=1$. Schinzel proved his result by showing that the term a^n-b^n was divisible by at least two primitive divisors. To prove this result he appealed to an Aurifeuillian factorization of Φ_n. Rotkiewicz [29] extended Schinzel's argument to treat Lucas numbers and then Schinzel [32], [33], [34] in a sequence of articles gave conditions under which Lehmer numbers possess at least two primitive divisors and so under which (1.3) holds with $n+1$ in place of $n-1$, see also [21]. In 1975 Stewart [37] proved that if $\varkappa$ is a positive real number with $\varkappa<1/\log 2$, then $P(a^n-b^n)/n$ tends to infinity with n provided that n runs through those integers with at most $\varkappa \log\log n$ distinct prime factors, see also [15]. Stewart [38] in the case that α and β are real and Shorey and Stewart [36] in the case that α and β are not real generalized this work to Lucas and Lehmer sequences. Let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero relatively prime integers with α/β not a root of unity. For any positive integer n let $\omega(n)$ denote the number of distinct prime factors of n and put $q(n)=2^{\omega(n)}$, the number of square-free divisors of n. Further let $\varphi(n)$ be the number of positive integers less than or equal to n and coprime with n. They showed, recall (1.4), if $n(>3)$ has at most $\varkappa \log\log n$ distinct prime factors then

$$P(\Phi_n(\alpha,\beta)) > C\frac{\varphi(n)\log n}{q(n)}, \tag{1.6}$$

where C is a positive number which is effectively computable in terms of α, β and $\varkappa$ only. The proofs depend on lower bounds for linear forms in the logarithms of algebraic numbers in the complex case when α and β are real and in the p-adic case otherwise.

The purpose of the present paper is to answer in the affirmative the question posed by Schinzel [31] and to prove Erdős' conjecture in the wider context of Lucas and Lehmer numbers.

THEOREM 1.1. *Let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero integers and α/β is not a root of unity. There exists a positive number C, which is effectively computable in terms of $\omega(\alpha\beta)$ and the discriminant of $\mathbb{Q}(\alpha/\beta)$, such that, for $n>C$,*

$$P(\Phi_n(\alpha,\beta)) > n\exp\left(\frac{\log n}{104\log\log n}\right). \tag{1.7}$$

Our result, with the aid of (1.4) gives an improvement of (1.1)–(1.3) and (1.6), answers the question of Schinzel and proves the conjecture of Erdős. Specifically, if a and b are integers with $a>b>0$, then

$$P(a^n-b^n) > n\exp\left(\frac{\log n}{104\log\log n}\right) \tag{1.8}$$

for n sufficiently large in terms of the number of distinct prime factors of ab. We remark that the factor 104 which occurs on the right-hand side of (1.7) has no arithmetical significance. Instead it is determined by the current quality of the estimates for linear forms in p-adic logarithms of algebraic numbers. In fact we could replace 104 by any number strictly larger than $14e^2$. The proof depends upon estimates for linear forms in the logarithms of algebraic numbers in the complex and the p-adic cases. In particular it depends upon a result of Yu [48], where improvements upon the dependence on the parameter p in the lower bounds for linear forms in p-adic logarithms of algebraic numbers are established. This allows us to estimate directly the order of primes dividing $\Phi_n(\alpha,\beta)$. The estimates are non-trivial for small primes and, coupled with an estimate from below for $|\Phi_n(\alpha,\beta)|$, they allow us to show that we must have a large prime divisor of $\Phi_n(\alpha,\beta)$ since otherwise the total non-archimedean contribution from the primes does not balance that of $|\Phi_n(\alpha,\beta)|$. By contrast for the proof of (1.6), a much weaker assumption on the greatest prime factor is imposed and it leads to the conclusion that then $\Phi_n(\alpha,\beta)$ is divisible by many small primes. This part of the argument from [36] and [38] was also employed in Murata and Pomerance's [27] proof of (1.5) and in estimates of Stewart [40] for the greatest square-free factor of $\tilde{u}_n$.

My initial proof of the conjecture of Erdős utilized an estimate for linear forms in p-adic logarithms established by Yu [47]. In order to treat also Lucas and Lehmer numbers, however, I need the more refined estimate obtained in [48], see §3.

For any non-zero integer x let $\mathrm{ord}_p x$ denote the p-adic order of x. Our next result follows from a special case of Lemma 4.3 of this paper. Lemma 4.3 yields a crucial step in the proof of Theorem 1.1. An unusual feature of the proof of Lemma 4.3 is that we artificially inflate the number of terms which occur in the p-adic linear form in logarithms which appear in the argument. We have chosen to highlight it in the integer case.

THEOREM 1.2. *Let a and b be integers with $a>b>0$. There exists a number C_1, which is effectively computable in terms of $\omega(ab)$, such that if p is a prime number which does not divide ab and which exceeds C_1, and n is an integer with $n\geqslant 2$, then*

$$\mathrm{ord}_p(a^n-b^n)<p\exp\left(-\frac{\log p}{52\log\log p}\right)\log a+\mathrm{ord}_p\, n. \tag{1.9}$$

If a and b are integers with $a>b>0$, n is an integer with $n\geqslant 2$ and p is an odd prime number which does not divide ab and exceeds C_1, then

$$\mathrm{ord}_p(a^{p-1}-b^{p-1})<p\exp\left(-\frac{\log p}{52\log\log p}\right)\log a.$$

Yamada [46], using a refinement of an estimate of Bugeaud and Laurent [7] for linear forms in two p-adic logarithms, proved that there is a positive number C_2, which is effectively computable in terms of $\omega(a)$, such that

$$\operatorname{ord}_p(a^{p-1}-1) < C_2 \frac{p}{(\log p)^2} \log a. \tag{1.10}$$

By following our proof of Theorem 1.1 and using (1.10) in place of Lemma 4.3 it is possible to show that there exist positive numbers C_3, C_4 and C_5, which are effectively computable in terms of $\omega(a)$, such that if n exceeds C_3 then

$$P(a^n-1) > C_4 \varphi(n)(\log n \log\log n)^{1/2}$$

and so, by Theorem 328 of [19],

$$P(a^n-1) > C_5 n \left(\frac{\log n}{\log\log n}\right)^{1/2}. \tag{1.11}$$

This gives an alternative proof of the conjecture of Erdős, although the lower bound (1.11) is weaker than the bound (1.8).

Acknowledgements. The research for this paper was done in part during visits to the Hong Kong University of Science and Technology, Institut des Hautes Études Scientifiques and the Erwin Schrödinger International Institute for Mathematical Physics, and I would like to express my gratitude to these institutions for their hospitality. In addition I wish to thank Professor Kunrui Yu for helpful remarks concerning the presentation of this article and for our extensive discussions on estimates for linear forms in p-adic logarithms which led to [48].

2. Preliminary lemmas

Let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero integers and α/β is not a root of unity. We shall assume, without loss of generality, that

$$|\alpha| \geqslant |\beta|.$$

Observe that

$$\alpha = \frac{\sqrt{r}+\sqrt{s}}{2} \quad \text{and} \quad \beta = \frac{\sqrt{r}-\sqrt{s}}{2},$$

where r and s are non-zero integers with $|r| \neq |s|$. Further $\mathbb{Q}(\alpha/\beta) = \mathbb{Q}(\sqrt{rs})$. Note that $(\alpha^2-\beta^2)^2 = rs$, and we may write rs in the form $m^2 d$, with m a positive integer and d a square-free integer so that $\mathbb{Q}(\sqrt{rs}) = \mathbb{Q}(\sqrt{d})$.

For any algebraic number γ let $h(\gamma)$ denote the absolute logarithmic height of γ. In particular if $a_0(x-\gamma_1) \dots (x-\gamma_d) \in \mathbb{Z}[x]$ is the minimal polynomial of γ over $\mathbb{Z}$, then

$$h(\gamma) = \frac{1}{d}\left(\log a_0 + \sum_{j=1}^{d} \log \max\{1, |\gamma_j|\}\right).$$

Notice that

$$\alpha\beta\left(x-\frac{\alpha}{\beta}\right)\left(x-\frac{\beta}{\alpha}\right) = \alpha\beta x^2-(\alpha^2+\beta^2)x+\alpha\beta = \alpha\beta x^2-((\alpha+\beta)^2-2\alpha\beta)x+\alpha\beta$$

is a polynomial with integer coefficients and so either α/β is rational or the polynomial is a multiple of the minimal polynomial of α/β. Therefore we have

$$h\left(\frac{\alpha}{\beta}\right) \leqslant \log|\alpha|. \tag{2.1}$$

We first record a result describing the prime factors of $\Phi_n(\alpha, \beta)$.

LEMMA 2.1. *Suppose that $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime. If $n>4$ and $n \notin \{6, 12\}$ then $P(n/(3,n))$ divides $\Phi_n(\alpha,\beta)$ to at most the first power. All other prime factors of $\Phi_n(\alpha,\beta)$ are congruent to* $\pm 1 \pmod n$.

Proof. This is Lemma 6 of [38]. □

Let K be a finite extension of $\mathbb{Q}$ and let $\wp$ be a prime ideal in the ring of algebraic integers $\mathcal{O}_K$ of K. Let $\mathcal{O}_\wp$ consist of 0 and the non-zero elements α of K for which $\wp$ has a non-negative exponent in the canonical decomposition of the fractional ideal generated by α into prime ideals. Then let P be the unique prime ideal of $\mathcal{O}_\wp$ and put $\overline{K}_\wp = \mathcal{O}_\wp/P$. Further for any α in $\mathcal{O}_\wp$ we let $\bar{\alpha}$ be the image of α under the residue class map that sends α to $\alpha+P$ in $\overline{K}_\wp$.

Our next result is motivated by work of Lucas [25] and Lehmer [23]. Let p be an odd prime and d be an integer coprime with p. Recall that the Legendre symbol (d/p) is 1 if d is a quadratic residue modulo p and -1 otherwise.

LEMMA 2.2. *Let d be a square-free integer different from* 1, *θ be an algebraic integer of degree* 2 *over $\mathbb{Q}$ in $\mathbb{Q}(\sqrt{d})$ and let θ' denote the algebraic conjugate of θ over $\mathbb{Q}$. Suppose that p is a prime which does not divide $2\theta\theta'$. Let $\wp$ be a prime ideal of the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$ lying above p. The order of $\overline{\theta/\theta'}$ in $\left(\overline{\mathbb{Q}(\sqrt{d})_\wp}\right)^\times$ is a divisor of* 2 *if p divides $(\theta^2-(\theta')^2)^2$ and a divisor of $p-(d/p)$ otherwise.*

Proof. We first note that θ and θ' are p-adic units. If p divides $(\theta^2-(\theta')^2)^2$ then either p divides $(\theta-\theta')^2$ or p divides $\theta+\theta'$ and in both cases $(\theta/\theta')^2 \equiv 1 \pmod \wp$. Hence the order of $\overline{\theta/\theta'}$ divides 2.

Thus we may suppose that p does not divide $2\theta\theta'(\theta^2-(\theta')^2)^2$ and, in particular, $p\nmid d$. Since

$$2\theta=(\theta+\theta')+(\theta-\theta') \quad \text{and} \quad 2\theta'=(\theta+\theta')-(\theta-\theta'), \tag{2.2}$$

we see, on raising both sides of the above equations to the pth power and subtracting, that $2^p(\theta^p-(\theta')^p)-2(\theta-\theta')^p$ is $p(\theta-\theta')$ times an algebraic integer. Hence, since p is odd,

$$\frac{\theta^p-(\theta')^p}{\theta-\theta'}\equiv(\theta-\theta')^{p-1} \pmod{p}.$$

But

$$(\theta-\theta')^{p-1}=((\theta-\theta')^2)^{(p-1)/2}\equiv\left(\frac{(\theta-\theta')^2}{p}\right) \pmod{p}$$

and

$$\left(\frac{(\theta-\theta')^2}{p}\right)=\left(\frac{d}{p}\right),$$

so

$$\frac{\theta^p-(\theta')^p}{\theta-\theta'}\equiv\left(\frac{d}{p}\right) \pmod{p}. \tag{2.3}$$

By raising both sides of equation (2.2) to the pth power and adding, we find that

$$\frac{\theta^p+(\theta')^p}{\theta+\theta'}\equiv(\theta+\theta')^{p-1} \pmod{p},$$

and, since $((\theta+\theta')^2/p)=1$,

$$\frac{\theta^p+(\theta')^p}{\theta+\theta'}\equiv 1 \pmod{p}. \tag{2.4}$$

If $(d/p)=-1$, then adding (2.3) and (2.4) we find that

$$2\frac{\theta^{p+1}-(\theta')^{p+1}}{\theta^2-(\theta')^2}\equiv 0 \pmod{p}.$$

Hence, since p does not divide $2\theta\theta'(\theta^2-(\theta')^2)^2$,

$$\left(\frac{\theta}{\theta'}\right)^{p+1}\equiv 1 \pmod{\wp}$$

and the result follows. If $(d/p)=1$ then subtracting (2.3) and (2.4) we find that

$$2\theta\theta'\frac{\theta^{p-1}-(\theta')^{p-1}}{\theta^2-(\theta')^2}\equiv 0 \pmod{p}.$$

Thus, since p does not divide $2\theta\theta'(\theta^2-(\theta')^2)^2$,

$$\left(\frac{\theta}{\theta'}\right)^{p-1}\equiv 1 \pmod{\wp}$$

and this completes the proof. □

We remark that it is also possible to prove Lemma 2.2 by exploiting the fact that $\overline{\theta/\theta'}$ is in the subgroup of $\big(\overline{\mathbb{Q}(\sqrt{d})_\wp}\big)^\times$ of elements of norm 1.

Let ℓ and n be integers with $n\geqslant 1$ and for each real number x let $\pi(x,n,\ell)$ denote the number of primes not greater than x and congruent to ℓ modulo n. We require a version of the Brun–Titchmarsh theorem, see [18, Theorem 3.8].

LEMMA 2.3. *If* $1\leqslant n<x$ *and* $(n,\ell)=1$ *then*

$$\pi(x,n,\ell)<\frac{3x}{\varphi(n)\log(x/n)}.$$

Our next result gives an estimate for the primes p below a given bound which occur as the norm of an algebraic integer in the ring of algebraic integers of $\mathbb{Q}(\alpha/\beta)$.

LEMMA 2.4. *Let* $d\neq 1$ *be a square-free integer and let* p_k *denote the* k*-th smallest prime of the form* $N\pi_k=p_k$, *where* N *denotes the norm from* $\mathbb{Q}(\sqrt{d})$ *to* $\mathbb{Q}$ *and* π_k *is an algebraic integer in* $\mathbb{Q}(\sqrt{d})$. *Let* ε *be a positive real number. There is a positive number* C, *which is effectively computable in terms of* ε *and* d, *such that if* k *exceeds* C *then*

$$\log p_k<(1+\varepsilon)\log k.$$

Proof. Let $K=\mathbb{Q}(\sqrt{d})$ and denote the ring of algebraic integers of K by $\mathcal{O}_K$. A prime p is the norm of an element π of $\mathcal{O}_K$ provided that it is representable as the value of the primitive quadratic form $q_K(x,y)$ given by

$$\begin{cases} x^2-dy^2, & \text{if } d\not\equiv 1 \pmod 4,\\ x^2+xy+\left(\dfrac{1-d}{4}\right)y^2, & \text{if } d\equiv 1 \pmod 4.\end{cases}$$

By [16, Chapter VII, (2.14)], a prime p is represented by $q_K(x,y)$ if and only if p is not inert in K and the prime ideals $\wp$ of $\mathcal{O}_K$ above p have trivial narrow class in the narrow ideal class group of K. Let K_H be the strict Hilbert class field of K. Since K_H is normal over K and G, the Galois group of K_H over K, is isomorphic with the narrow ideal class group of K it follows that $|G|=h^+$, the strict ideal class number of K, see Theorem 7.1.2 of [10]. The prime ideals $\wp$ of $\mathcal{O}_K$ which do not ramify in K_H and which are principal, are the only prime ideals of $\mathcal{O}_K$ which do not ramify in K_H and which split completely in K_H, see Theorem 7.1.3 of [10]. These prime ideals may be counted by the Chebotarev density theorem. Let

$$\left[\frac{K_H/K}{\wp}\right]$$

denote the conjugacy class of Frobenius automorphisms corresponding to prime ideals P of $\mathcal{O}_{K_H}$ above $\wp$. In particular, for each conjugacy class C of G we define $\pi_C(x,K_H/K)$

to be the cardinality of the set of prime ideals $\wp$ of $\mathcal{O}_K$ which are unramified in K_H, for which

$$\left[\frac{K_H/K}{\wp}\right] = C$$

and for which $N_{K/\mathbb{Q}}\wp \leqslant x$. Denote by C_0 the conjugacy class consisting of the identity element of G. Note that the number of inert primes p of $\mathcal{O}_K$ for which $N_{K/\mathbb{Q}}\, p \leqslant x$ is at most $x^{1/2}$. Thus the number of primes p up to x for which p is the norm of an element π of $\mathcal{O}_K$ is bounded from below by

$$\pi_{C_0}\left(x, \frac{K_H}{K}\right) - x^{1/2}. \tag{2.5}$$

It follows from Theorems 1.3 and 1.4 of [22] that there is a positive number C_1, which is effectively computable in terms of d, such that for x greater than C_1 the quantity (2.5) exceeds

$$\frac{x}{2h^+ \log x}.$$

Further

$$\frac{x}{2h^+ \log x} > k$$

when x is at least $4h^+ k \log k$ and

$$\frac{k}{\log k} > 4h^+. \tag{2.6}$$

Thus, provided (2.6) holds and x exceeds C_1,

$$p_k < 4h^+ k \log k. \tag{2.7}$$

Our result now follows from (2.7) on taking logarithms. □

3. Estimates for linear forms in p-adic logarithms of algebraic numbers

Let $\alpha_1, ..., \alpha_n$ be non-zero algebraic numbers and put $K = \mathbb{Q}(\alpha_1, ..., \alpha_n)$ and $d = [K:\mathbb{Q}]$. Let $\wp$ be a prime ideal of the ring $\mathcal{O}_K$ of algebraic integers in K lying above the prime number p. Denote by $e_\wp$ the ramification index of $\wp$ and by $f_\wp$ the residue class degree of $\wp$. For α in K with $\alpha \neq 0$ let $\operatorname{ord}_\wp \alpha$ be the exponent to which $\wp$ divides the principal fractional ideal generated by α in K and put $\operatorname{ord}_\wp 0 = \infty$. For any positive integer m let $\zeta_m = e^{2\pi i/m}$ and put $\alpha_0 = \zeta_{2^u}$ where $\zeta_{2^u} \in K$ and $\zeta_{2^{u+1}} \notin K$.

Suppose that $\alpha_1, ..., \alpha_n$ are multiplicatively independent $\wp$-adic units in K. Let $\bar{\alpha}_0, \bar{\alpha}_1, ..., \bar{\alpha}_n$ be the images of $\alpha_0, \alpha_1, ..., \alpha_n$, respectively, under the residue class map at $\wp$ from the ring of $\wp$-adic integers in K onto the residue class field $\overline{K}_\wp$ at $\wp$. For any set

X let $|X|$ denote its cardinality. Let $\langle\bar{\alpha}_0, \bar{\alpha}_1, ..., \bar{\alpha}_n\rangle$ be the subgroup of $(\overline{K}_\wp)^\times$ generated by $\bar{\alpha}_0, \bar{\alpha}_1, ..., \bar{\alpha}_n$. We define δ by

$$\delta = 1, \quad \text{if } [K(\alpha_0^{1/2}, \alpha_1^{1/2}, ..., \alpha_n^{1/2}) : K] < 2^{n+1},$$

and

$$\delta = \frac{p^{f_\wp} - 1}{|\langle\bar{\alpha}_0, \bar{\alpha}_1, ..., \bar{\alpha}_n\rangle|},$$

if

$$[K(\alpha_0^{1/2}, \alpha_1^{1/2}, ..., \alpha_n^{1/2}) : K] = 2^{n+1}. \tag{3.1}$$

Denote $\log\max\{x, e\}$ by $\log^* x$.

LEMMA 3.1. *Let $p \geqslant 5$ be a prime and let $\wp$ be an unramified prime ideal of $\mathcal{O}_K$ lying above p. Let $\alpha_1, ..., \alpha_n$ be multiplicatively independent $\wp$-adic units. Let $b_1, ..., b_n$ be integers, not all zero, and put*

$$B = \max\{2, |b_1|, ..., |b_n|\}.$$

Then

$$\operatorname{ord}_\wp(\alpha_1^{b_1} ... \alpha_n^{b_n} - 1) < C h(\alpha_1) ... h(\alpha_n) \max\{\log B, (n+1)(5.4n + \log d)\},$$

where

$$C = 376(n+1)^{1/2}\left(7e\frac{p-1}{p-2}\right)^n d^{n+2} \log^* d \log(e^4(n+1)d) \max\left\{\frac{p^{f_p}}{\delta}\left(\frac{n}{f_p \log p}\right)^n, e^n f_p \log p\right\}.$$

Proof. We apply the main theorem of [48] and in [48, (1.18)] we take $C_1(n, d, \wp, a)h^{(1)}$ in place of the minimum. Further [48, (1.17)] holds since our result is symmetric in the b_i's. Next we note that, as $\wp$ is unramified and $p \geqslant 5$, we may take

$$c^{(1)} = 1794, \quad a^{(1)} = 7\frac{p-1}{p-2}, \quad a_0^{(1)} = 2 + \log 7 \quad \text{and} \quad a_1^{(1)} = a_2^{(1)} = 5.25.$$

We remark that condition (3.1) ensures that we may take $\{\theta_1, ..., \theta_n\}$ to be $\{\alpha_1, ..., \alpha_n\}$. Finally the explicit version of Dobrowolski's theorem due to Voutier [42] allows us to replace the first term in the maximum defining $h^{(1)}$ by $\log B$. Therefore we find that

$$\operatorname{ord}_\wp(\alpha_1^{b_1} ... \alpha_n^{b_n} - 1) < C_1 h(\alpha_1) ... h(\alpha_n) \max\{\log B, G_1, (n+1) f_\wp \log p\},$$

where

$$G_1 = (n+1)((2 + \log 7)n + 5.25 + \log((2 + \log 7)n + 5.25) + \log d),$$

and

$$C_1 = 1794\left(7\left(\frac{p-1}{p-2}\right)\right)^n \frac{(n+1)^{n+1}}{n!} \frac{d^{n+2}\log^* d}{2^u(f_\wp \log p)^2}$$
$$\times \max\left\{\frac{p^{f_\wp}}{\delta}\left(\frac{n}{f_\wp \log p}\right)^n, e^n f_\wp \log p\right\} \max\{\log(e^4(n+1)d), f_\wp \log p\}.$$

Note that $2^u \geqslant 2$ and $f_\wp \log p \geqslant \log 5$. Further, by Stirling's formula, see [1, 6.1.38],

$$\frac{(n+1)^{n+1}}{n!} \leqslant \frac{e^{n+1}(n+1)^{1/2}}{\sqrt{2\pi}}$$

and so

$$\mathrm{ord}_\wp(\alpha_1^{b_1} \dots \alpha_n^{b_n} - 1) < C_2 h(\alpha_1) \dots h(\alpha_n) \max\left\{\frac{\log B}{\log 5}, \frac{G_1}{\log 5}, n+1\right\}, \tag{3.2}$$

where

$$C_2 = \frac{1794}{2} \frac{e}{\sqrt{2\pi}} (n+1)^{1/2} \left(7e\frac{p-1}{p-2}\right)^n d^{n+2} \log^* d$$
$$\times \max\left\{\frac{p^{f_\wp}}{\delta}\left(\frac{n}{f_\wp \log p}\right)^n, e^n f_\wp \log p\right\} \frac{\log(e^4(n+1)d)}{\log 5}. \tag{3.3}$$

We next observe that

$$G_1 \leqslant (n+1)(5.4n + \log d)$$

and, as a consequence,

$$\max\left\{\frac{\log B}{\log 5}, \frac{G_1}{\log 5}, n+1\right\} = \max\left\{\frac{\log B}{\log 5}, \frac{(n+1)(5.4n+\log d)}{\log 5}\right\}. \tag{3.4}$$

The result now follows from (3.2)–(3.4). □

The key new feature in Yu's main theorem in [48], as compared with his estimate in [47], is the introduction of the factor δ. It is the presence of δ in the statement of Lemma 3.1 that allows us to extend our argument to the case when $\mathbb{Q}(\alpha/\beta)$ is different from $\mathbb{Q}$.

4. Further preliminaries

Let $(\alpha+\beta)^2$ and $\alpha\beta$ be non-zero integers with α/β not a root of unity. We may suppose that $|\alpha| \geqslant |\beta|$. Since there is a positive number c_0 which exceeds 1 such that $|\alpha| \geqslant c_0$, we deduce from [39, Lemma 3], see also [35, Lemmas 1 and 2], that there is a positive number c_1 which we may suppose exceeds $(\log c_0)^{-1}$ such that, for $n>0$,

$$\log 2 + n\log|\alpha| \geqslant \log|\alpha^n - \beta^n| \geqslant (n - c_1\log(n+1))\log|\alpha|. \tag{4.1}$$

The proof of (4.1) depends upon an estimate for a linear form in the logarithms of two algebraic numbers due to Baker [2].

For any positive integer n let $\mu(n)$ denote the Möbius function of n. It follows from (1.4) that

$$\Phi_n(\alpha,\beta)=\prod_{d\mid n}(\alpha^{n/d}-\beta^{n/d})^{\mu(d)}. \tag{4.2}$$

We may now deduce, following the approach of [35] and [39], our next result.

LEMMA 4.1. *There exists an effectively computable positive number c such that if $n>2$ then*

$$|\alpha|^{\varphi(n)-cq(n)\log n}\leqslant|\Phi_n(\alpha,\beta)|\leqslant|\alpha|^{\varphi(n)+cq(n)\log n}, \tag{4.3}$$

where $q(n)=2^{\omega(n)}$.

Proof. By (4.2),

$$\log|\Phi_n(\alpha,\beta)|=\sum_{d\mid n}\mu(d)\log|\alpha^{n/d}-\beta^{n/d}|,$$

and so, by (4.1),

$$\left|\log|\Phi_n(\alpha,\beta)|-\sum_{d\mid n}\mu(d)\frac{n}{d}\log|\alpha|\right|\leqslant\sum_{\substack{d\mid n\\ \mu(d)\neq 0}}c_1\log(n+1)\log|\alpha|,$$

since c_1 exceeds $(\log c_0)^{-1}$. Our result now follows. □

LEMMA 4.2. *There exists an effectively computable positive number c_2 such that if n exceeds c_2 then*

$$\log|\Phi_n(\alpha,\beta)|\geqslant\tfrac{1}{2}\varphi(n)\log|\alpha|. \tag{4.4}$$

Proof. For n sufficiently large

$$\varphi(n)>\frac{n}{2\log\log n}\quad\text{and}\quad q(n)<n^{1/\log\log n}.$$

Since $|\alpha|\geqslant c_0>1$, it follows from (4.3) that, if n is sufficiently large,

$$|\Phi_n(\alpha,\beta)|>|\alpha|^{\varphi(n)/2},$$

as required. □

LEMMA 4.3. *Let $n>1$ be an integer, let p be a prime which does not divide $\alpha\beta$ and let $\wp$ be a prime ideal of the ring of algebraic integers of $\mathbb{Q}(\alpha/\beta)$ lying above p which does not ramify. Then there exists a positive number C, which is effectively computable in terms of $\omega(\alpha\beta)$ and the discriminant of $\mathbb{Q}(\alpha/\beta)$, such that if p exceeds C then*

$$\operatorname{ord}_\wp\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) < p\exp\left(-\frac{\log p}{51.9\log\log p}\right)\log|\alpha|\log n.$$

Proof. Let $c_3, c_4, \ldots$ denote positive numbers which are effectively computable in terms of $\omega(\alpha\beta)$ and the discriminant of $\mathbb{Q}(\alpha/\beta)$. We remark that, since α/β is of degree at most 2 over $\mathbb{Q}$, the discriminant of $\mathbb{Q}(\alpha/\beta)$ determines the field $\mathbb{Q}(\alpha/\beta)$ and so knowing it one may compute the class number and regulator of $\mathbb{Q}(\alpha/\beta)$ as well as the strict Hilbert class field of $\mathbb{Q}(\alpha/\beta)$ and the discriminant of this field. Further let p be a prime which does not divide $6d\alpha\beta$, where d is defined as in the first paragraph of §2.

Put $K=\mathbb{Q}(\alpha/\beta)$ and

$$\alpha_0 = \begin{cases} i, & \text{if } i \in K, \\ -1, & \text{otherwise.} \end{cases}$$

Let v be the largest integer for which

$$\frac{\alpha}{\beta} = \alpha_0^j \theta^{2^v}, \tag{4.5}$$

with $0 \leqslant j \leqslant 3$ and θ in K. To see that there is a largest such integer, we first note that either there is a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$, the ring of algebraic integers of K, lying above a prime q which occurs to a positive exponent in the principal fractional ideal generated by α/β, or α/β is a unit. In the former case $h(\alpha/\beta) \geqslant 2^{v-1}\log q$ and in the latter case, since α/β is not a root of unity, there is a positive number c_3, see [12], such that $h(\alpha/\beta) \geqslant 2^v c_3$.

Notice from (4.5) that

$$h\left(\frac{\alpha}{\beta}\right) = 2^v h(\theta). \tag{4.6}$$

Further, by Kummer theory, see Lemma 3 of [3],

$$[K(\alpha_0^{1/2}, \theta^{1/2}) : K] = 4. \tag{4.7}$$

Furthermore, since $p \nmid \alpha\beta$ and α and β are algebraic integers,

$$\operatorname{ord}_\wp\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) \leqslant \operatorname{ord}_\wp\left(\left(\frac{\alpha}{\beta}\right)^{4n} - 1\right). \tag{4.8}$$

For any real number x let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x. Put

$$k = \left\lfloor \frac{\log p}{51.8\log\log p} \right\rfloor. \tag{4.9}$$

Then, for $p>c_4$, we find that $k\geqslant 2$ and

$$\max\left\{p\left(\frac{k}{\log p}\right)^k, e^k\log p\right\} = p\left(\frac{k}{\log p}\right)^k. \tag{4.10}$$

Our proof splits into two cases. We shall first suppose that $\mathbb{Q}(\alpha/\beta)=\mathbb{Q}$ so that α and β are integers. For any positive integer j with $j\geqslant 2$ let p_j denote the $(j-1)$-th smallest prime which does not divide $p\alpha\beta$. We put

$$m = n2^{v+2} \tag{4.11}$$

and

$$\alpha_1 = \frac{\theta}{p_2 \dots p_k}.$$

Then

$$\theta^m - 1 = \left(\frac{\theta}{p_2 \dots p_k}\right)^m p_2^m \dots p_k^m - 1 = \alpha_1^m p_2^m \dots p_k^m - 1 \tag{4.12}$$

and, by (4.5), (4.8), (4.11) and (4.12),

$$\operatorname{ord}_p\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) \leqslant \operatorname{ord}_p(\alpha_1^m p_2^m \dots p_k^m - 1). \tag{4.13}$$

Note that $\alpha_1, p_2, \dots, p_k$ are multiplicatively independent since α/β is not a root of unity and $p_2, \dots, p_k$ are primes which do not divide $p\alpha\beta$. Further, since $p_2, \dots, p_k$ are different from p and p does not divide $\alpha\beta$, we see that $\alpha_1, p_2, \dots, p_k$ are p-adic units.

We now apply Lemma 3.1 with $\delta=1$, $d=1$, $f_\wp=1$ and $n=k$ to conclude that

$$\begin{aligned}\operatorname{ord}_p(\alpha_1^m p_2^m \dots p_k^m - 1) \leqslant c_5(k+1)^3\left(7e\frac{p-1}{p-2}\right)^k \max\left\{p\left(\frac{k}{\log p}\right)^k, e^k\log p\right\} \\ \times(\log m)h(\alpha_1)\log p_2 \dots \log p_k.\end{aligned} \tag{4.14}$$

Put

$$t = \omega(\alpha\beta).$$

Let q_i denote the ith prime number. Note that

$$p_k \leqslant q_{k+t+1},$$

and thus

$$\log p_2 + \dots + \log p_k \leqslant (k-1)\log q_{k+t+1}.$$

By the prime number theorem with error term, for $k>c_6$,

$$\log p_2 + \dots + \log p_k \leqslant 1.001(k-1)\log k. \tag{4.15}$$

By the arithmetic geometric mean inequality,

$$\log p_2 \dots \log p_k \leqslant \left(\frac{\log p_2 + \dots + \log p_k}{k-1}\right)^{k-1},$$

and so, by (4.15),

$$\log p_2 \dots \log p_k \leqslant (1.001 \log k)^{k-1}. \tag{4.16}$$

Since $h(\alpha_1) \leqslant h(\theta) + \log p_2 \dots p_k$, it follows from (4.15) that

$$h(\alpha_1) \leqslant c_7 h(\theta) k \log k. \tag{4.17}$$

Further $m = 2^{v+2} n$ is at most $n^{2^{v+2}}$ and so, by (2.1) and (4.6),

$$h(\theta) \log m \leqslant 4h\left(\frac{\alpha}{\beta}\right) \log n \leqslant 4 \log |\alpha| \log n. \tag{4.18}$$

Thus, by (4.10), (4.13), (4.14), (4.16), (4.17) and (4.18),

$$\operatorname{ord}_p\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) < c_8 k^4 \left(7e \frac{p-1}{p-2} 1.001 \frac{k \log k}{\log p}\right)^k p \log |\alpha| \log n.$$

Therefore, by (4.9), for $p > c_9$,

$$\operatorname{ord}_p\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) < p e^{-\log p / 51.9 \log \log p} \log |\alpha| \log n. \tag{4.19}$$

We now suppose that $[\mathbb{Q}(\alpha/\beta):\mathbb{Q}] = 2$. Let $\pi_2, \dots, \pi_k$ be elements of $\mathcal{O}_K$ with the property that $N(\pi_i) = p_i$, where N denotes the norm from K to $\mathbb{Q}$ and where p_i is the $(i-1)$-th smallest rational prime number of this form which does not divide $2dp\alpha\beta$. We now put $\theta_i = \pi_i / \pi_i'$, where π_i' denotes the algebraic conjugate of π_i in $\mathbb{Q}(\alpha/\beta)$. Notice that p does not divide $\pi_i \pi_i' = p_i$ and if p does not divide $(\pi_i - \pi_i')^2$ then

$$\left(\frac{(\pi_i - \pi_i')^2}{p}\right) = \left(\frac{d}{p}\right),$$

since $\mathbb{Q}(\alpha/\beta) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\pi_i)$. Thus, by Lemma 2.2, the order of θ_i in $(\overline{\mathbb{Q}(\alpha/\beta)_\wp})^\times$ is a divisor of 2 if p divides $(\pi_i^2 - (\pi_i')^2)^2$ and a divisor of $p - (d/p)$ otherwise. Since p is odd and p does not divide d we conclude that the order of θ_i in $(\overline{\mathbb{Q}(\alpha/\beta)_\wp})^\times$ is a divisor of $p - (d/p)$.

Put

$$\alpha_1 = \frac{\theta}{\theta_2 \dots \theta_k}. \tag{4.20}$$

Then

$$\theta^m - 1 = \left(\frac{\theta}{\theta_2 \dots \theta_k}\right)^m \theta_2^m \dots \theta_k^m - 1$$

and, by (4.5), (4.8), (4.11) and (4.20),

$$\operatorname{ord}_\wp\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) \leqslant \operatorname{ord}_\wp(\alpha_1^m \theta_2^m \dots \theta_k^m - 1). \tag{4.21}$$

Observe that $\alpha_1, \theta_2, ..., \theta_k$ are multiplicatively independent since α/β is not a root of unity, $p_2, ..., p_k$ are primes which do not divide $\alpha\beta$ and the principal prime ideals $[\pi_i]$ for $i=2, ..., k$ do not ramify as $p\nmid 2d$. Further, since $p_2, ..., p_k$ are different from p and p does not divide $\alpha\beta$, we see that $\alpha_1, \theta_2, ..., \theta_k$ are $\wp$-adic units.

Notice that

$$K(\alpha_0^{1/2}, \theta^{1/2}, \theta_2^{1/2}, ..., \theta_k^{1/2}) = K(\alpha_0^{1/2}, \alpha_1^{1/2}, \theta_2^{1/2}, ..., \theta_k^{1/2}).$$

Furthermore

$$[K(\alpha_0^{1/2}, \theta^{1/2}, \theta_2^{1/2}, ..., \theta_k^{1/2}) : K] = 2^{k+1}, \tag{4.22}$$

since otherwise, by (4.7) and Kummer theory, see Lemma 3 of [3], there is an integer i with $2 \leqslant i \leqslant k$ and integers $j_0, ..., j_{i-1}$ with $0 \leqslant j_b \leqslant 1$ for $b=0, ..., i-1$ and an element γ of K for which

$$\theta_i = \alpha_0^{j_0} \theta^{j_1} \theta_2^{j_2} \dots \theta_{i-1}^{j_{i-1}} \gamma^2. \tag{4.23}$$

But the order of the prime ideal $[\pi_i]$ on the left-hand side of (4.23) is 1 whereas the order on the right-hand side of (4.23) is even, which is a contradiction. Thus (4.22) holds.

Since p does not divide the discriminant of K and $[K:\mathbb{Q}]=2$, either p splits, in which case $f_\wp=1$ and $(d/p)=1$, or p is inert, in which case $f_\wp=2$ and $(d/p)=-1$, see [20]. Observe that if $(d/p)=1$ then

$$\frac{p^{f_\wp}}{\delta} \leqslant p. \tag{4.24}$$

Let us now determine $|\langle \bar{\alpha}_0, \bar{\theta}, \bar{\theta}_2, ..., \bar{\theta}_k \rangle|$ in the case $(d/p)=-1$. By our earlier remarks, the order of $\bar{\theta}_i$ is a divisor of $p+1$ for $i=2, ..., k$. Further, by (4.5), since $N(\alpha/\beta)=1$, we find that $N(\theta)=\pm 1$ and so $N(\theta^2)=1$. By Hilbert's Theorem 90, see e.g. [9, Theorem 14.35], $\theta^2=\varrho/\varrho'$ where ϱ and ϱ' are conjugate algebraic integers in $\mathbb{Q}(\alpha/\beta)$. Note that we may suppose that the principal ideals $[\varrho]$ and $[\varrho']$ have no principal ideal divisors in common. Further, since p does not divide $\alpha\beta$ and since $(d/p)=-1$, $[p]$ is a principal prime ideal of $\mathcal{O}_K$ and we note that p does not divide $\varrho\varrho'$. It follows from Lemma 2.2 that the order of θ^2 in $(\overline{\mathbb{Q}(\alpha/\beta)_\wp})^\times$ is a divisor of $p+1$, and hence the order of θ is a divisor of $2(p+1)$. Since $\alpha_0^4=1$, we conclude that

$$|\langle \bar{\alpha}_0, \bar{\theta}, \bar{\theta}_2, ..., \bar{\theta}_k \rangle| \leqslant 2(p+1)$$

and so

$$\delta = \frac{p^2-1}{|\langle \bar{\alpha}_0, \bar{\theta}, \bar{\theta}_2, ..., \bar{\theta}_k \rangle|} \geqslant \frac{p-1}{2}. \tag{4.25}$$

We now apply Lemma 3.1 noting, by (4.24) and (4.25), that

$$\frac{p^{f_\wp}}{\delta} \leqslant \frac{2p^2}{p-1}.$$

Thus, by (4.10),

$$\mathrm{ord}_\wp(\alpha_1^m \theta_2^m ... \theta_k^m - 1) \leqslant c_{10}(k+1)^3 \left(7e\frac{p-1}{p-2}\right)^k 2^k p \left(\frac{k}{\log p}\right)^k (\log m) h(\alpha_1) h(\theta_2) ... h(\theta_k). \tag{4.26}$$

Notice that $\theta_i = \pi_i/\pi_i'$ and that $p_i(x-\pi_i/\pi_i')(x-\pi_i'/\pi_i) = p_i x^2 - (\pi_i^2 + (\pi_i')^2)x + p_i$ is the minimal polynomial of θ_i over the integers, since $[\pi_i]$ is unramified. Either the discriminant of $\mathbb{Q}(\alpha/\beta)$ is negative, in which case $|\pi_i| = |\pi_i'|$, or it is positive, in which case there is a fundamental unit $\varepsilon > 1$ in $\mathcal{O}_K$. We may replace π_i by $\pi_i \varepsilon^u$ for any integer u and so without loss of generality we may suppose that $p_i^{1/2} \leqslant |\pi_i| \leqslant p_i^{1/2}\varepsilon$ and consequently that $p_i^{1/2}\varepsilon^{-1} \leqslant |\pi_i'| \leqslant p_i^{1/2}$. Therefore

$$h(\theta_i) \leqslant \tfrac{1}{2}\log p_i \varepsilon^2 = \tfrac{1}{2}\log p_i + \log \varepsilon \quad \text{for } d > 0$$

and

$$h(\theta_i) \leqslant \tfrac{1}{2}\log p_i \quad \text{for } d < 0.$$

Let us put

$$R = \begin{cases} \log \varepsilon & \text{for } d > 0, \\ 0 & \text{for } d < 0. \end{cases}$$

Then

$$h(\theta_i) \leqslant \tfrac{1}{2}\log p_i + R \tag{4.27}$$

for $i = 2, ..., k$. In a similar fashion we find that

$$h(\theta_2 ... \theta_k) \leqslant \tfrac{1}{2}\log p_2 ... p_k + R, \tag{4.28}$$

and so

$$h(\alpha_1) \leqslant h(\theta) + \tfrac{1}{2}\log p_2 ... p_k + R. \tag{4.29}$$

Put

$$t_1 = \omega(2dp\alpha\beta).$$

Let q_i denote the ith prime number which is representable as the norm of an element of $\mathcal{O}_K$. Note that

$$p_k \leqslant q_{k+t_1},$$

and thus

$$\log p_2 + ... + \log p_k \leqslant (k-1) \log q_{k+t_1}.$$

Therefore, by Lemma 2.4, for $k > c_{11}$,

$$\log p_2 + ... + \log p_k \leqslant 1.0005(k-1) \log k \tag{4.30}$$

and so, as for the proof of (4.16),

$$\log p_2 \ldots \log p_k \leqslant (1.0005 \log k)^{k-1}.$$

Accordingly, since $p_k \geqslant k$, for $k > c_{12}$,

$$2^{k-1} h(\theta_2) \ldots h(\theta_k) \leqslant (\log p_2 + 2R) \ldots (\log p_k + 2R) \leqslant (1.001 \log k)^{k-1}. \tag{4.31}$$

Furthermore, as for the proof of (4.17) and (4.18), we find that from (4.29),

$$h(\alpha_1) \leqslant c_{13} h(\theta) k \log k \tag{4.32}$$

and, from (2.1), (4.6) and (4.11),

$$h(\theta) \log m \leqslant 8 \log |\alpha| \log n. \tag{4.33}$$

Thus by (4.21), (4.26), (4.29), (4.31), (4.32) and (4.33),

$$\operatorname{ord}_\wp \left(\left(\frac{\alpha}{\beta} \right)^n - 1 \right) < c_{14} k^4 \left(7e \left(\frac{p-1}{p-2} \right) 1.001 \frac{k \log k}{\log p} \right)^k p \log |\alpha| \log n. \tag{4.34}$$

Therefore, by (4.9), for $p > c_{15}$ we again obtain (4.19) and the result follows. □

5. Proof of Theorem 1.1

Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of $\omega(\alpha\beta)$ and the discriminant of $\mathbb{Q}(\alpha/\beta)$. Let g be the greatest common divisor of $(\alpha+\beta)^2$ and $\alpha\beta$. Note that $\varphi(n)$ is even for $n > 2$ and that

$$\Phi_n(\alpha, \beta) = g^{\varphi(n)/2} \Phi_n(\alpha_1, \beta_1),$$

where $\alpha_1 = \alpha/\sqrt{g}$ and $\beta_1 = \beta/\sqrt{g}$. Further $(\alpha_1+\beta_1)^2$ and $\alpha_1\beta_1$ are coprime and plainly

$$P(\Phi_n(\alpha,\beta)) \geqslant P(\Phi_n(\alpha_1,\beta_1)).$$

Therefore we may assume, without loss of generality, that $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime non-zero integers.

By Lemma 4.2, there exists c_1 such that if n exceeds c_1 then

$$\log|\Phi_n(\alpha,\beta)| \geqslant \tfrac{1}{2}\varphi(n)\log|\alpha|. \tag{5.1}$$

On the other hand,

$$\Phi_n(\alpha,\beta) = \prod_{p \mid \Phi_n(\alpha,\beta)} p^{\operatorname{ord}_p \Phi_n(\alpha,\beta)}. \tag{5.2}$$

If p divides $\Phi_n(\alpha,\beta)$ then, by (1.4), p does not divide $\alpha\beta$, and so

$$\operatorname{ord}_p \Phi_n(\alpha,\beta) \leqslant \operatorname{ord}_\wp\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right), \tag{5.3}$$

where $\wp$ is a prime ideal of $\mathcal{O}_K$ lying above p. By Lemma 2.1, if p divides $\Phi_n(\alpha,\beta)$ and p is not $P(n/(3,n))$, then p is at least $n-1$ and thus, for $n>c_2$, by Lemma 4.3,

$$\operatorname{ord}_\wp\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) < p\exp\left(-\frac{\log p}{51.9\log\log p}\right)\log|\alpha|\log n. \tag{5.4}$$

Put

$$P_n = P(\Phi_n(\alpha,\beta)).$$

Then, by (5.2) and Lemma 2.1,

$$\log|\Phi_n(\alpha,\beta)| \leqslant \log n + \sum_{\substack{p \leqslant P_n \\ p \nmid n}} \log p \operatorname{ord}_p \Phi_n(\alpha,\beta). \tag{5.5}$$

Comparing (5.1) and (5.5) and using (5.3) and (5.4) we find that, for $n>c_3$,

$$\varphi(n)\log|\alpha| < \sum_{\substack{p \leqslant P_n \\ p \nmid n}} c_4(\log p)p\exp\left(-\frac{\log p}{51.9\log\log p}\right)\log|\alpha|\log n.$$

Hence

$$\frac{\varphi(n)}{\log n} < (\pi(P_n,n,1)+\pi(P_n,n,-1))P_n\exp\left(-\frac{\log P_n}{51.95\log\log P_n}\right),$$

and, by Lemma 2.3,

$$c_5\frac{\varphi(n)}{\log n} < \frac{P_n^2}{\varphi(n)\log(P_n/n)}\exp\left(-\frac{\log P_n}{51.95\log\log P_n}\right).$$

Since $\varphi(n) > c_6 n/\log\log n$,

$$P_n > n\exp\left(\frac{\log n}{104\log\log n}\right)$$

for $n>c_7$, as required.

6. Proof of Theorem 1.2

Since p does not divide ab,

$$\mathrm{ord}_p(a^n-b^n)=\mathrm{ord}_p\left(\left(\frac{a}{g}\right)^n-\left(\frac{b}{g}\right)^n\right),$$

where g is the greatest common divisor of a and b. Thus we may assume, without loss of generality, that a and b are coprime. Put $u_n=a^n-b^n$ for $n=1,2,...$, and let $\ell=\ell(p)$ be the smallest positive integer for which p divides u_ℓ. Certainly p divides u_{p-1}. Further, as in the proof of Lemma 3 of [38], if n and m are positive integers then

$$(u_n,u_m)=u_{(n,m)}.$$

Thus if p divides u_n then p divides $u_{(n,\ell)}$. By the minimality of ℓ we see that $(n,\ell)=\ell$, so that ℓ divides n. In particular, ℓ divides $p-1$. Furthermore, by (1.4), we see that

$$\mathrm{ord}_p\, u_\ell=\mathrm{ord}_p\,\Phi_\ell(a,b).$$

If ℓ divides n then, by Lemma 2 of [38],

$$\left(\frac{u_n}{u_\ell},u_\ell\right)\quad\text{divides}\quad\frac{n}{\ell},\tag{6.1}$$

and so

$$\mathrm{ord}_p\, u_{p-1}=\mathrm{ord}_p\, u_\ell.\tag{6.2}$$

Suppose that p divides $\Phi_n(a,b)$. Then p divides u_n and so ℓ divides n. Put $n=t\ell p^k$ with $(t,p)=1$ and k a non-negative integer. Since $\Phi_n(a,b)$ divides $u_n/u_{n/t}$ for $t>1$, we see from (6.1), as $(t,p)=1$, that $t=1$. Thus $n=\ell p^k$. For any positive integer m,

$$\frac{u_{mp}}{u_m}=pb^{(m-1)p}+\binom{p}{2}b^{(m-2)p}u_m+...+u_m^{p-1},$$

and if p is not 2 and p divides u_m then $\mathrm{ord}_p(u_{mp}/u_m)=1$. It then follows that if p is an odd prime then

$$\mathrm{ord}_p\,\Phi_{\ell p^k}(a,b)=1\quad\text{for } k=1,2,\dots.$$

If n is a positive integer not divisible by $\ell=\ell(p)$, then $|u_n|_p=1$. On the other hand, if p is odd and ℓ divides n, then

$$|u_n|_p=|u_\ell|_p\left|\frac{n}{\ell}\right|_p.\tag{6.3}$$

It now follows from (6.2) and (6.3) and the fact that $\ell\leqslant p-1$ that, if p is an odd prime and ℓ divides n, then

$$|u_n|_p=|u_{p-1}|_p\,|n|_p.\tag{6.4}$$

Therefore, if p is an odd prime and n is a positive integer, then

$$\mathrm{ord}_p(a^n-b^n)\leqslant\mathrm{ord}_p(a^{p-1}-b^{p-1})+\mathrm{ord}_p\, n,\tag{6.5}$$

and our result now follows from (6.5) on taking $n=p-1$ in Lemma 4.3.

References

[1] Abramowitz, M. & Stegun, I. A., *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. National Bureau of Standards Applied Mathematics Series, 55. U.S. Government Printing Office, Washington, DC, 1972.

[2] Baker, A., A sharpening of the bounds for linear forms in logarithms. *Acta Arith.*, 21 (1972), 117–129.

[3] Baker, A. & Stark, H. M., On a fundamental inequality in number theory. *Ann. of Math.*, 94 (1971), 190–199.

[4] Bang, A. S., Taltheoretiske undersøgelser. *Tidsskrift for Mat.*, 4 (1886), 70–80, 130–137.

[5] Bilu, Y., Hanrot, G. & Voutier, P. M., Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539 (2001), 75–122.

[6] Birkhoff, G. D. & Vandiver, H. S., On the integral divisors of a^n-b^n. *Ann. of Math.*, 5 (1904), 173–180.

[7] Bugeaud, Y. & Laurent, M., Minoration effective de la distance p-adique entre puissances de nombres algébriques. *J. Number Theory*, 61 (1996), 311–342.

[8] Carmichael, R. D., On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math.*, 15 (1913/14), 30–70.

[9] Cohn, H., *A Classical Invitation to Algebraic Numbers and Class Fields*. Springer, New York, 1978.

[10] — *Introduction to the Construction of Class Fields*. Cambridge Studies in Advanced Mathematics, 6. Cambridge University Press, Cambridge, 1985.

[11] Dickson, L. E., *History of the Theory of Numbers*. Vol. I: *Divisibility and Primality*. Chelsea, New York, 1966.

[12] Dobrowolski, E., On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34 (1979), 391–401.

[13] Durst, L. K., Exceptional real Lehmer sequences. *Pacific J. Math.*, 9 (1959), 437–441.

[14] Erdős, P., Some recent advances and current problems in number theory, in *Lectures on Modern Mathematics*, Vol. III, pp. 196–244. Wiley, New York, 1965.

[15] Erdős, P. & Shorey, T. N., On the greatest prime factor of 2^p-1 for a prime p and other expressions. *Acta Arith.*, 30 (1976), 257–265.

[16] Fröhlich, A. & Taylor, M. J., *Algebraic Number Theory*. Cambridge Studies in Advanced Mathematics, 27. Cambridge University Press, Cambridge, 1993.

[17] Gel′fond, A. O., *Transcendental and Algebraic Numbers*. Dover, New York, 1960.

[18] Halberstam, H. & Richert, H. E., *Sieve Methods*. London Mathematical Society Monographs, 4. Academic Press, London–New York, 1974.

[19] Hardy, G. H. & Wright, E. M., *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford, 2008.

[20] Hecke, E., *Lectures on the Theory of Algebraic Numbers*. Graduate Texts in Mathematics, 77. Springer, New York, 1981.

[21] Juricevic, R., *Lehmer Numbers with at least 2 Primitive Divisors*. Ph. D. Thesis, University of Waterloo, Waterloo, ON, 2008.

[22] Lagarias, J. C. & Odlyzko, A. M., Effective versions of the Chebotarev density theorem, in *Algebraic Number Fields*: *L-functions and Galois Properties* (Durham, 1975), pp. 409–464. Academic Press, London, 1977.

[23] Lehmer, D. H., An extended theory of Lucas' functions. *Ann. of Math.*, 31 (1930), 419–448.

[24] Lucas, E., Sur les rapports qui existent entre la théorie des nombres et le calcul intégral. *C. R. Acad. Sci. Paris*, 82 (1876), 1303–1305.

[25] — Théorie des fonctions numériques simplement périodiques. *Amer. J. Math.*, 1 (1878), 184–240.

[26] Matijasevich, Yu. V., The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191 (1970), 279–282 (Russian); English translation in *Soviet Math. Dokl.*, 11 (1970), 354–358.

[27] Murata, L. & Pomerance, C., On the largest prime factor of a Mersenne number, in *Number Theory*, CRM Proc. Lecture Notes, 36, pp. 209–218. Amer. Math. Soc., Providence, RI, 2004.

[28] Murty, R. & Wong, S., The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences, in *Number Theory for the Millennium*, III (Urbana, IL, 2000), pp. 43–54. A K Peters, Natick, MA, 2002.

[29] Rotkiewicz, A., On Lucas numbers with two intrinsic prime divisors. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, 10 (1962), 229–232.

[30] Schinzel, A., The intrinsic divisors of Lehmer numbers in the case of negative discriminant. *Ark. Mat.*, 4 (1962), 413–416.

[31] — On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Philos. Soc.*, 58 (1962), 555–562.

[32] — On primitive prime factors of Lehmer numbers. I. *Acta Arith.*, 8 (1962/1963), 213–223.

[33] — On primitive prime factors of Lehmer numbers. II. *Acta Arith.*, 8 (1962/1963), 251–257.

[34] — On primitive prime factors of Lehmer numbers. III. *Acta Arith.*, 15 (1968), 49–70.

[35] — Primitive divisors of the expression $A^n - B^n$ in algebraic number fields. *J. Reine Angew. Math.*, 268/269 (1974), 27–33.

[36] Shorey, T. N. & Stewart, C. L., On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. II. *J. London Math. Soc.*, 23 (1981), 17–23.

[37] Stewart, C. L., The greatest prime factor of $a^n - b^n$. *Acta Arith.*, 26 (1974/75), 427–433.

[38] — On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers. *Proc. London Math. Soc.*, 35 (1977), 425–447.

[39] — Primitive divisors of Lucas and Lehmer numbers, in *Transcendence Theory: Advances and Applications* (Cambridge, 1976), pp. 79–92. Academic Press, London, 1977.

[40] — On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. III. *J. London Math. Soc.*, 28 (1983), 211–217.

[41] Stewart, C. L. & Yu, K., On the *abc* conjecture. II. *Duke Math. J.*, 108 (2001), 169–181.

[42] Voutier, P. M., An effective lower bound for the height of algebraic numbers. *Acta Arith.*, 74 (1996), 81–95.

[43] — Primitive divisors of Lucas and Lehmer sequences. II. *J. Théor. Nombres Bordeaux*, 8 (1996), 251–274.

[44] — Primitive divisors of Lucas and Lehmer sequences. III. *Math. Proc. Cambridge Philos. Soc.*, 123 (1998), 407–419.

[45] Ward, M., The intrinsic divisors of Lehmer numbers. *Ann. of Math.*, 62 (1955), 230–236.

[46] Yamada, T., A note on the paper by Bugeaud and Laurent "Minoration effective de la distance p-adique entre puissances de nombres algébriques". *J. Number Theory*, 130 (2010), 1889–1897.

[47] Yu, K., p-adic logarithmic forms and group varieties. III. *Forum Math.*, 19 (2007), 187–280.

[48] — p-adic logarithmic forms and a problem of Erdős. *Acta Math.*, 211 (2013), 315–382.

[49] Zsigmondy, K., Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3 (1892), 265–284.

Cameron L. Stewart
Department of Pure Mathematics
University of Waterloo
Waterloo, ON N2L 3G1
Canada
cstewart@uwaterloo.ca

Received February 2, 2012
Received in revised form November 16, 2012