ON DIVISORS OF LUCAS AND LEHMER NUMBERS

C.L. STEWART

Abstract. Let \( u_n \) be the \( n \)-th 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.

1. Introduction

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

\[
u_n = (\alpha^n - \beta^n)/(\alpha - \beta) \quad \text{for } n \geq 0.
\]

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 Matijasevic [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 \( \alpha \) and \( \beta \) are real and \( n > 12 \) then

\[
P(u_n) \geq n - 1.
\]

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 \( n > 2 \)

\[
P(a^n - b^n) \geq n + 1,
\]

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

In 1930 Lehmer [22] 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 \( \alpha/\beta \) not a root of unity and, for \( n > 0 \), put

\[
\tilde{u}_n = \begin{cases} 
(\alpha^n - \beta^n)/(\alpha - \beta) & \text{for } n \text{ odd}, \\
(\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{for } n \text{ even}.
\end{cases}
\]

2000 Mathematics Subject Classification. 11B39, 11J86.

Key words and phrases. greatest prime factor, recurrence sequences, Lucas numbers.

Research supported in part by the Canada Research Chairs Program and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.
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 $\alpha$ and $\beta$ are real then for $n > 18$,

$$P(\bar{u}_n) \geq n - 1, \quad (3)$$

and four years later Durst [13] observed that (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 $(\alpha - \beta)^2 u_2 \cdots u_{n-1}$. Similarly $p$ is said to be a primitive divisor of a Lehmer number $\bar{u}_n$ if $p$ divides $\bar{u}_n$ but does not divide $(\alpha^2 - \beta^2)^2 \bar{u}_3 \cdots \bar{u}_{n-1}$. For any integer $n > 0$ and any pair of complex numbers $\alpha$ and $\beta$, we denote the $n$-th cyclotomic polynomial in $\alpha$ and $\beta$ by $\Phi_n(\alpha, \beta)$, so

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

where $\zeta$ is a primitive $n$-th 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 Lemma 6 of [38], if, in addition, $(\alpha + \beta)^2$ and $\alpha \beta$ are coprime non-zero integers, $\alpha / \beta$ is not a root of unity and $n > 4$ 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 to all other prime factors of $\Phi_n(\alpha, \beta)$ are congruent to 1 (mod $n$) in the case that $\alpha$ and $\beta$ are coprime integers.

Since

$$\alpha^n - \beta^n = \prod_{d | n} \Phi_d(\alpha, \beta), \quad (4)$$

$\Phi_1(\alpha, \beta) = \alpha - \beta$ 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 $\bar{u}_n$ then $p$ divides $\Phi_n(\alpha, \beta)$. Further, a primitive divisor of a Lucas number $u_n$ or Lehmer number $\bar{u}_n$ is not a divisor of $n$ and so it is congruent to $\pm 1$ (mod $n$). Estimates [3], [2] and [3] follow as consequences of the fact that the $n$-th term of the sequences in question possesses a primitive divisor. It was not until 1962 that this approach was extended to the case where $\alpha$ and $\beta$ are not real by Schinzel [31]. He proved, by means of an estimate for linear forms in two logarithms of algebraic numbers due to Gelfond [17], that there is a positive number $C$, which is effectively computable in terms of $\alpha$ and $\beta$, such that if $n$ exceeds $C$ then $\bar{u}_n$ possesses a primitive divisor. In 1974 Schinzel [35] employed an estimate of Baker [3] 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 $\alpha$ and $\beta$, and in 1977 Stewart [39] showed $C_0$ could be taken to be $e^{4.524 \cdot 10^6}$. This was subsequently refined by Voutier [42] 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 $n$-th term of a Lucas or Lehmer sequence has a primitive divisor. Thus (1) and (3) hold for $n > 30$ without the restriction that $\alpha$ and $\beta$ be real.

In 1962 Schinzel [30] asked if there exists a pair of integers $a, b$ with $ab$ different from $\pm 2e^2$ and $\pm e^h$ with $h \geq 2$ 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 [11]. They proved, subject to the abc conjecture, that if $\varepsilon$ 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 that $n$ is sufficiently large in terms of $a$, $b$ and $\varepsilon$. In 2004 Murata and Pomerance [27] proved, subject to the Generalized Riemann Hypothesis, that
\[
P(2^n - 1) > \frac{n^{4/3}}{\log \log n}
\]
for a set of positive integers $n$ of asymptotic density 1.

The first unconditional refinement of (2) was obtained by Schinzel [30] in 1962. He proved that if $a$ and $b$ are coprime and $ab$ is a square or twice a square then
\[
P(a^n - b^n) \geq 2n + 1
\]
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 2 primitive divisors. To prove this result he appealed to an Aurifeuillian factorization of $\Phi_n$. 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 2 primitive divisors and so under which (3) holds with $n + 1$ in place of $n - 1$, see also [21]. In 1975 Stewart [37] proved that if $\kappa$ is a positive real number with $\kappa < 1/\log 2$ then $P(a^n - b^n)/n$ tends to infinity with $n$ provided that $n$ runs through those integers with at most $\kappa \log \log n$ distinct prime factors, see also [15]. Stewart [38] in the case that $\alpha$ and $\beta$ are real and Shorey and Stewart [36] in the case that $\alpha$ and $\beta$ are not real generalized this work to Lucas and Lehmer sequences. Let $\alpha$ and $\beta$ be complex numbers such that $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero relatively prime integers with $\alpha/\beta$ 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 [11], if $n > 3$ has at most $\kappa \log \log n$ distinct prime factors then
\[
P(\Phi_n(\alpha, \beta)) > C(\varphi(n) \log n)/q(n),
\]
where $C$ is a positive number which is effectively computable in terms of $\alpha$, $\beta$ and $\kappa$ only. The proofs depend on lower bounds for linear forms in the logarithms of algebraic numbers in the complex case when $\alpha$ and $\beta$ 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 [30] and to prove Erdős’ conjecture in the wider context of Lucas and Lehmer numbers.

**Theorem 1.** Let $\alpha$ and $\beta$ be complex numbers such that $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero integers and $\alpha/\beta$ 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 $n > C$,
\[
P(\Phi_n(\alpha, \beta)) > n \exp(\log n/104 \log \log n).
\]
Our result, with the aid of (4) gives an improvement of (1), (2), (3) and (6), answers the question of Schinzel and proves the conjecture of Erdős. Specifically, if $a$ and $b$ are integers with $a > b > 0$ then

$$P(a^n - b^n) > n \exp(\log n/104 \log \log n),$$

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 (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 $14 e^2$. The proof depends upon estimates for linear forms in the logarithms of algebraic numbers in the complex and the $p$-adic case. In particular it depends upon [18] 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 (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 [39] and in estimates of Stewart [40] for the greatest square-free factor of $\tilde{u}_n$.

For any non-zero integer $x$ let $\ord_p x$ denote the $p$-adic order of $x$. Our next result follows from a special case of Lemma 8 of this paper. Lemma 8 yields a crucial step in the proof of Theorem 1. An unusual feature of the proof of Lemma 8 is that we artificially inflate the number of terms which occur in the $p$-adic linear form in logarithms which appears in the argument. We have chosen to highlight it in the integer case.

**Theorem 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 $n \geq 2$ then

$$\ord_p (a^n - b^n) < p \exp(- \log p / 52 \log \log p) \log a + \ord_p n.$$  

(9)

If $a$ and $b$ are integers with $a > b > 0$, $p$ is an odd prime number which does not divide $ab$ and $n \geq 2$ then, as in the proof of Theorem 2,

$$\ord_p (a^n - b^n) \leq \ord_p (a^{p-1} - b^{p-1}) + \ord_p n.$$  

In particular if $p$ exceeds $C_1$ then

$$\ord_p (a^{p-1} - b^{p-1}) < p \exp(- \log p / 52 \log \log p) \log a.$$  

Yamada [46], by making use of 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

$$\ord_p (a^{p-1} - 1) < C_2 (p / (\log p)^2) \log a.$$  

(10)
By following our proof of Theorem 1 and using (10) in place of Lemma 8 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

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

and so, by Theorem 328 of [19],

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

(11)

This gives an alternative proof of the conjecture of Erdős, although the lower bound
(11) is weaker than the bound (8).

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

$$|\alpha| \geq |\beta|.$$ 

Observe that

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

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

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

$$\alpha\beta(x - \alpha/\beta)(x - \beta/\alpha) = \alpha\beta x^2 - (\alpha^2 + \beta^2)x + \alpha\beta = \alpha\beta x^2 - ((\alpha + \beta)^2 - 2\alpha\beta)x + \alpha\beta$$

is a polynomial with integer coefficients and so either $\alpha/\beta$ is rational or the poly-
nomial is a multiple of the minimal polynomial of $\alpha/\beta$. Therefore we have

$$h(\alpha/\beta) \leq \log |\alpha|. \quad (12)$$

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

**Lemma 1.** Suppose that $(\alpha + \beta)^2$ and $\alpha\beta$ are coprime. If $n > 4$ and $n \neq 6, 12$ then
$P(n/(3n))$ 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 $\mathfrak{p}$ be a prime ideal in the ring of algebraic integers $\mathcal{O}_K$ of $K$. Let $\mathcal{O}_\mathfrak{p}$ consist of 0 and the non-zero elements $\alpha$ of $K$ for which $\mathfrak{p}$ has a non-negative exponent in the canonical decomposition of the fractional ideal generated by $\alpha$ into prime ideals. Then let $P$ be the unique prime ideal of $\mathcal{O}_\mathfrak{p}$ and put $K_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/P$. Further for any $\alpha$ in $\mathcal{O}_\mathfrak{p}$ we let $\overline{\alpha}$ be the image of $\alpha$ under the residue class map that sends $\alpha$ to $\alpha + P$ in $K_\mathfrak{p}$.

Our next result is motivated by work of Lucas [25] and Lehmer [22].

**Lemma 2.** Let $d$ be a square-free integer different from 1, $\theta$ be an algebraic integer of degree 2 over $\mathbb{Q}$ in $\mathbb{Q}(\sqrt{d})$ and let $\theta'$ denote the algebraic conjugate of $\theta$ over $\mathbb{Q}$. Suppose that $p$ is a prime which does not divide $2\theta\theta'$. Let $\mathfrak{p}$ be a prime ideal of the ring of algebraic integers of $\mathbb{Q}(\sqrt{d})$ lying above $p$. The order of $\theta/\theta'$ in $(\mathbb{Q}(\sqrt{d}))^\times$ 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 $\theta$ and $\theta'$ 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 $(\theta/\theta')^2 \equiv 1 \pmod{\mathfrak{p}}$. Thus the order of $\theta/\theta'$ 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

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

we see, on raising both sides of the above equations to the $p$-th 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

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

and

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

so

$$\frac{\theta^p - \theta'^p}{\theta - \theta'} \equiv \left(\frac{d}{p}\right) \pmod{p}.$$  \hspace{1cm} (14)

By raising both sides of equation (14) to the $p$-th power and adding we find that

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

and since $\left(\frac{(\theta + \theta')^2}{p}\right) = 1$,

$$\frac{\theta^p + \theta'^p}{\theta + \theta'} \equiv 1 \pmod{p}.$$  \hspace{1cm} (15)

If $\left(\frac{d}{p}\right) = -1$ then adding (14) and (15) 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 $2\theta\theta'(\theta^2 - \theta'^2)^2$,

$$(\theta/\theta')^{p+1} \equiv 1 \pmod{\mathfrak{p}}$$
and the result follows. If \( \left( \frac{d}{p} \right) = 1 \) then subtracting \([14]\) and \([15]\) we find that
\[
2\theta \theta \frac{\theta'p^{-1} - \theta'^{-1}}{\theta'^2 - \theta'^2} \equiv 0 \pmod{p}
\]
hence, since \( p \) does not divide \( 2\theta \theta'(\theta'^2 - \theta'^2) \),
\[
(\theta/\theta')^{p^{-1}} \equiv 1 \pmod{\varphi}
\]
and this completes the proof. \( \square \)

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

**Lemma 3.** If \( 1 \leq n < x \) and \( (n,\ell) = 1 \) then
\[
\pi(x,n,\ell) < \frac{x}{\varphi(n)} \log(x/n)).
\]

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 4.** Let \( d \) be a squarefree integer with \( d \neq 1 \) 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 \( \pi_k \) is an algebraic integer in \( \mathbb{Q}(\sqrt{d}) \). Let \( \epsilon \) be a positive real number. There is a positive number \( C \), which is effectively computable in terms of \( \epsilon \) and \( d \), such that if \( k \) exceeds \( C \) then
\[
\log p_k < (1 + \epsilon) \log k.
\]

**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 \( \pi \) of \( \mathcal{O}_K \) provided that it is representable as the value of the primitive quadratic form \( q_K(x,y) \) given by \( x^2 - dy^2 \) if \( d \neq 1 \pmod{4} \) and \( x^2 + xy + \left( \frac{1-d}{4} \right)y^2 \) if \( d \equiv 1 \pmod{4} \). By \([14\, \text{Chapter VII, (2.14)]} \), a prime \( p \) is represented by \( q_K(x,y) \) if and only if \( p \) is not inert in \( K \) and all prime ideals \( \varphi \) of \( \mathcal{O}_K \) above \( p \) have trivial narrow class in the narrow ideal class group of \( K \). Let \( H \) be the strict Hilbert class field of \( K \). \( H/K \) is normal over \( K \) and the Galois group of \( H/K \) over \( K \), is isomorphic with the narrow ideal class group of \( K \) and so \( |G| = h^+ \), the strict ideal class number of \( K \), see Theorem 7.1.2 of \([10]\). The prime ideals \( \varphi \) 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 \( \left[ \mathcal{K}_H/K \varphi \right] \) denote the conjugacy class of Frobenius automorphisms corresponding to prime ideals \( P \) of \( \mathcal{O}_{K_H} \) above \( \varphi \). 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 \( \varphi \) of \( \mathcal{O}_K \) which are unramified in \( K_H \), for which \( \left[ \mathcal{K}_H/K \varphi \right] \right. = C \) and for which \( N_{K/Q} \varphi \leq x \). 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 \( N_{K/Q} p \leq x \) is at most \( x^{1/2} \). Thus the number of primes \( p \) up to \( x \) for which \( p \) is the norm of an element \( \pi \) of \( \mathcal{O}_K \) is bounded from below by
\[
\pi_{C_0}(x,K_H/K) \leq x^{1/2}.
\]
It follows from Theorem 1.3 and 1.4 of 23 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 (16) exceeds
\[
\frac{x}{2h^+ \log x}.
\]
Further
\[
\frac{x}{2h^+ \log x} > k
\]
when $x$ is at least $4h^+ k \log k$ and
\[
k/ \log k > 4h^+.
\]
Thus, provided (17) holds and $x$ exceeds $C_1$,
\[
p_k < 4h^+ k \log k.
\]
Our result now follows from (18) on taking logarithms. \qed

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

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and put $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ 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 $e_\wp, f_\wp$ the ramification index of $\wp$ and by $\delta_\wp$ the residue class degree of $\wp$. For $\alpha$ in $K$ with $\alpha \neq 0$ let $\ord_\wp \alpha$ be the exponent to which $\wp$ divides the principal fractional ideal generated by $\alpha$ in $K$ and put $\ord_\wp 0 = \infty$.

For any positive integer $m$ let $\zeta_m = e^{2\pi i / m}$ and put $\alpha_0 = \zeta_{2^n}$ where $\zeta_{2^n} \in K$ and $\zeta_{2^{n+1}} \notin K$.

Suppose that $\alpha_1, \ldots, \alpha_n$ are multiplicatively independent $\wp$-adic units in $K$. Let $\overline{\alpha_0, \alpha_1, \ldots, \alpha_n}$ be the images of $\alpha_0, \alpha_1, \ldots, \alpha_n$ under the residue class map at $\wp$ from the ring of $\wp$-adic integers in $K$ onto the residue class field $K_\wp$ at $\wp$. For any set $X$ let $|X|$ denote its cardinality. Let $\langle \overline{\alpha_0, \alpha_1, \ldots, \alpha_n} \rangle$ be the subgroup of $(K_\wp)^\times$ generated by $\overline{\alpha_0, \alpha_1, \ldots, \alpha_n}$. We define $\delta$ by

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

and

$\delta = (p^{f_\wp} - 1)/|\langle \overline{\alpha_0, \alpha_1, \ldots, \alpha_n} \rangle|$ if $[K(\alpha_0^{1/2}, \alpha_1^{1/2}, \ldots, \alpha_n^{1/2}) : K] = 2^{n+1}$. (19)

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

$B = \max(2, |b_1|, \ldots, |b_n|)$. Then

$\ord_\wp (\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1) < Ch(\alpha_1) \cdots h(\alpha_n) \max(\log B, (n+1)(5.4n + \log d))$

where

$C = 376(n+1)^{1/2} \left(7e^{p-1} \sqrt{2} \right) d^{n+2} \log^* d \log(e^4(n+1)d) \cdot \max \left( \frac{p^{f_\wp}}{\delta}, \left( \frac{n}{f_\wp \log p} \right)^n, e^n f_\wp \log p \right)$.
Proof: We apply the Main Theorem of [18] and in (1.16) we take $C_1(n, d, \varphi, a)h(1)$ in place of the minimum. Further (1.15) holds since our result is symmetric in the $b_i$’s. Next we note that, since $\varphi$ is unramified and $p \geq 5$, we may take $c(1) = 1794$, $a^{(1)} = 7^{p-1}/p$, $a_0^{(1)} = 2 + \log 7$ and $a_0^{(1)} = a_2^{(1)} = 5.25$. We remark that condition (19) ensures that we may take $\{\theta_1, \ldots, \theta_n\}$ to be $\{\alpha_1, \ldots, \alpha_n\}$. Finally the explicit version of Dobrowolski’s Theorem due to Voutier [44] allows us to replace the first term in the maximum defining $h(1)$ by $\log B$. Therefore we find that
\[
\operatorname{ord}_\varphi(a_1^{b_1} \cdots a_n^{b_n} - 1) < C_1 h(\alpha_1) \cdots h(\alpha_n) \max(\log B, G_1, (n + 1)f_\varphi \log p)
\]
where
\[
G_1 = (n + 1)(2 + \log 7)n + 5.25 + \log((2 + \log 7)n + 5.25) + \log d
\]
and, on denoting $\log \max(x, e)$ by $\log^* x$,
\[
C_1 = 1794 \left(7 \left(\frac{p - 1}{p - 2}\right)^n \frac{n + 1}{n!} \right) \frac{d^{n+2} \log^* d}{2^n (f_\varphi \log p)^2} \\
\cdot \max\left(\frac{p^f_\varphi}{\delta} \left(\frac{n}{f_\varphi \log p}\right)^n, e^n f_\varphi \log p\right) \cdot \max(\log(e^4(n + 1)d), f_\varphi \log p).
\]
Note that $2^n \geq 2$ and $f_\varphi \log p \geq \log 5$. Further, by Stirling’s formula, see 6.1.38 of [11],
\[
\frac{(n + 1)^{n+1}}{n!} \leq e^{n+1}(n + 1)^{1/2}
\]
and so
\[
\operatorname{ord}_\varphi(a_1^{b_1} \cdots a_n^{b_n} - 1) < C_2 h(\alpha_1) \cdots h(\alpha_n) \max\left(\frac{\log B}{\log 5}, \frac{G_1}{\log 5}, n + 1\right) 
\]
where
\[
C_2 = 1794 \left(7e \frac{p - 1}{p - 2}\right) \frac{n^{n+1}}{n!} \frac{d^{n+2} \log^* d}{2^n (f_\varphi \log p)^2} \\
\max\left(\frac{p^f_\varphi}{\delta} \left(\frac{n}{f_\varphi \log p}\right)^n, e^n f_\varphi \log p\right) \frac{(\log(e^4(n + 1)d))}{\log 5}.
\]
We next observe that
\[
G_1 \leq (n + 1)(5.4n + \log d)
\]
and as a consequence
\[
\max\left(\frac{\log B}{\log 5}, \frac{G_1}{\log 5}, n + 1\right) = \max\left(\frac{\log B}{\log 5}, \frac{(n + 1)(5.4n + \log d)}{\log 5}\right).
\]
The result now follows from (20), (21) and (22). \hfill \Box

4. Further preliminaries

Let $(\alpha + \beta)^2$ and $\alpha \beta$ be non-zero integers with $\alpha/\beta$ not a root of unity. We may suppose that $|\alpha| \geq |\beta|$. Since there is a positive number $c_0$ which exceeds 1 such that $|\alpha| \geq c_0$ we deduce from Lemma 3 of [39], see also Lemmas 1 and 2 of [35], that there is a positive number $c_1$ which we may suppose exceeds $(\log c_0)^{-1}$ such that for $n > 0$
\[
\log 2 + n \log |\alpha| \geq \log |\alpha^n - \beta^n| \geq (n - c_1 \log(n + 1)) \log |\alpha|.
\]
The proof of (23) 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 (4) that
\[
\Phi_n(\alpha, \beta) = \prod_{d|n} (\alpha^{n/d} - \beta^{n/d})^{\mu(d)}.
\] (24)

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

**Lemma 6.** There exists an effectively computable positive number \( c \) such that if \( n > 2 \) then
\[
|\alpha|^{\varphi(n)} - cq(n) \log n \leq |\Phi_n(\alpha, \beta)| \leq |\alpha|^{\varphi(n)} + cq(n) \log n,
\] (25)

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

**Proof.** By (24)
\[
\log |\Phi_n(\alpha, \beta)| = \sum_{d|n} \mu(d) \log |\alpha^{n/d} - \beta^{n/d}|
\]
and so by (23)
\[
\left| \log |\Phi_n(\alpha, \beta)| - \sum_{d|n} \mu(d) \frac{n}{d} \log |\alpha| \right| \leq \sum_{d|n} \mu(d) \neq 0 c_1 \log(n+1) \log |\alpha|
\]
since \( c_1 \) exceeds \((\log c_0)^{-1}\). Our result now follows. \(\square\)

**Lemma 7.** There exists an effectively computable positive number \( c_1 \) such that if \( n \) exceeds \( c_1 \) then
\[
\log |\Phi_n(\alpha, \beta)| \geq \frac{\varphi(n)}{2} \log |\alpha|.
\] (26)

**Proof.** For \( n \) sufficiently large
\[
\varphi(n) > n/2 \log \log n \quad \text{and} \quad q(n) < n^{1/\log \log n}.
\]
Since \( |\alpha| \geq c_0 > 1 \) it follows from (25) that if \( n \) is sufficiently large
\[
|\Phi_n(\alpha, \beta)| > |\alpha|^{\varphi(n)/2},
\]
as required. \(\square\)

**Lemma 8.** Let \( n \) be an integer larger than 1, let \( p \) be a prime which does not divide \( \alpha \beta \) and let \( \omega \) 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
\[
\ord_p((\alpha/\beta)^n - 1) < p \exp(- \log p/51.9 \log \log p) \log |\alpha| \log n.
\]

**Proof.** Let \( c_1, c_2, \ldots \) denote positive numbers which are effectively computable in terms of \( \omega(\alpha\beta) \) and the discriminant of \( \mathbb{Q}(\alpha/\beta) \). We remark that since \( \alpha/\beta \) 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
\[
\alpha/\beta = \alpha_0^v \theta^{2^v},
\]
with $0 \leq j \leq 3$ and $\theta$ in $K$. To see that there is a largest such integer we first note that either there is a prime ideal $q$ of $O_K$, 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 $\alpha/\beta$ or $\alpha/\beta$ is a unit. In the former case $h(\alpha/\beta) \geq 2^{v-1} \log q$ and in the latter case, since $\alpha/\beta$ is not a root of unity, there is a positive number $c_1$, see [12], such that $h(\alpha/\beta) \geq 2^v c_1$.

Notice from (27) that
\[
h(\alpha/\beta) = 2^v h(\theta).
\]
Further, by Kummer theory, see Lemma 3 of [3],
\[
[K(\alpha_0^{1/2}, \theta^{1/2}) : K] = 4.
\]
Furthermore since $p \nmid \alpha \beta$ and $\alpha$ and $\beta$ are algebraic integers
\[
\ord_p((\alpha/\beta)^n - 1) \leq \ord_p((\alpha/\beta)^{4n} - 1).
\]

For any real number $x$ let $[x]$ denote the greatest integer less than or equal to $x$. Put
\[
k = \left\lfloor \frac{\log p}{51.8 \log \log p} \right\rfloor.
\]
Then, for $p > c_2$, we find that $k \geq 2$ and
\[
\max \left( p \left( \frac{k}{\log p} \right)^k, e^{k \log p} \right) = p \left( \frac{k}{\log p} \right)^k.
\]

Our proof splits into two cases. We shall first suppose that $\mathbb{Q}(\alpha/\beta) = \mathbb{Q}$ so that $\alpha$ and $\beta$ are integers. For any positive integer $j$ with $j \geq 2$ let $p_j$ denote the $j-1$-th smallest prime which does not divide $p\alpha \beta$. We put
\[
m = n2^{v+2}
\]
and
\[
\alpha_1 = \theta/p_2 \cdots p_k.
\]
Then
\[
\theta^m - 1 = \left( \frac{\theta}{p_2 \cdots p_k} \right)^m p_2^m \cdots p_k^m - 1 = \alpha_1^m p_2^m \cdots p_k^m - 1
\]
and by (27), (30), (33) and (34)
\[
\ord_p((\alpha/\beta)^n - 1) \leq \ord_p(\alpha_1^m p_2^m \cdots p_k^m - 1).
\]

Note that $\alpha_1, p_2, \ldots, p_k$ are multiplicatively independent since $\alpha/\beta$ is not a root of unity and $p_2, \ldots, p_k$ are primes which do not divide $p\alpha \beta$. Further, since $p_2, \ldots, p_k$ are different from $p$ and $p$ does not divide $\alpha \beta$, we see that $\alpha_1, p_2, \ldots, p_k$ are $p$-adic units.
We now apply Lemma 5 with $\delta = 1$, $d = 1$, $f_{\nu} = 1$ and $n = k$ to conclude that
\[
\text{ord}_p(\alpha m_1 p_2^m \cdots p_k^m - 1) \leq c_3(k + 1)^3 \log p \left(\frac{7e p - 1}{p - 2}\right)^k \max \left(p \left(\frac{k}{\log p}\right)^k, e^k\right) (\log m) h(\alpha_1) \log p_2 \cdots \log p_k.
\] (36)

Put
\[t = \omega(\alpha \beta).\]
Let $q_i$ denote the $i$-th prime number. Note that $p_k \leq q_k + t + 1$ and thus
\[
\log p_2 + \cdots + \log p_k \leq (k - 1) \log q_k + t + 1.
\]
By the prime number theorem with error term, for $k > c_4$, 
\[
\log p_2 + \cdots + \log p_k \leq 1.001(k - 1) \log k.
\] (37)

By the arithmetic geometric mean inequality
\[
\log p_2 \cdots \log p_k \leq \left(\frac{\log p_2 + \cdots + \log p_k}{k - 1}\right)^{k - 1}
\]
and so, by (37)
\[
\log p_2 \cdots \log p_k \leq (1.001 \log k)^{k - 1}.
\] (38)

Since $h(\alpha_1) \leq h(\theta) + \log p_2 \cdots p_k$ it follows from (37) that
\[
h(\alpha_1) \leq c_5 h(\theta) k \log k.
\] (39)

Further $m = 2^{v+2} n$ is at most $n^{2v+2}$ and so by (12) and (28)
\[
h(\theta) \log m \leq 4 h(\alpha/\beta) \log n \leq 4 \log |\alpha| \log n.
\] (40)

Thus, by (32), (35), (36), (38), (39) and (40),
\[
\text{ord}_p((\alpha/\beta)^n - 1) \leq c_6 k^4 \log p \left(\frac{7e p - 1}{p - 2}\right)^k \frac{k \log k}{\log p} p \log |\alpha| \log n.
\]

Therefore, by (31), for $p > c_7$
\[
\text{ord}_p((\alpha/\beta)^n - 1) < pe^{-\frac{\log p}{2\pi d p} \log |\alpha| \log n}.
\] (41)

We now suppose that $[\mathbb{Q}(\alpha/\beta) : \mathbb{Q}] = 2$. Let $\pi_2, \ldots, \pi_k$ be elements of $O_K$ with the property that $N(\pi_i) = p_i$ where $N$ denotes the norm from $K$ to $\mathbb{Q}$ and where $p_i$ is a rational prime number which does not divide $2d p \alpha \beta$. We now put $\theta_i = \pi_i / \pi_i'$ where $\pi_i'$ denotes the algebraic conjugate of $\pi_i$ in $\mathbb{Q}(\alpha/\beta)$. Notice that $p$ does not divide $\pi_i \pi_i'$ 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, the order of $\theta_i$ in $(\mathbb{Q}(\alpha/\beta)_{\nu})^\times$ is a divisor of 2 if $p$ divides $\pi_i^2 - \pi_i'^2$ and a divisor of $p - \left(\frac{d}{p}\right)$ otherwise. Since $p$ is
odd and $p$ does not divide $d$ we conclude that the order of $\theta_i$ in $(\mathbb{Q}(\alpha/\beta))_p^\times$ is a divisor of $p - \left(\frac{d}{p}\right)$.

Put

$$\alpha_1 = \theta/\theta_2 \cdots \theta_k.$$ (42)

Then

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

and, by (27), (30), (33) and (42),

$$\text{ord}_p((\alpha/\beta)^m - 1) \leq \text{ord}_p(\alpha_1^m \theta_2^m \cdots \theta_k^m - 1).$$ (43)

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

Notice that

$$K(\alpha_0^{1/2}, \theta_1^{1/2}, \theta_2^{1/2}, \ldots, \theta_k^{1/2}) = K(\alpha_0^{1/2}, \alpha_1^{1/2}, \theta_2^{1/2}, \ldots, \theta_k^{1/2}).$$ Further

$$[K(\alpha_0^{1/2}, \theta_1^{1/2}, \theta_2^{1/2}, \ldots, \theta_k^{1/2}) : K] = 2^{k+1},$$ (44)

since otherwise, by (29) and Kummer theory, see Lemma 3 of [3], there is an integer $i$ with $2 \leq i \leq k$ and integers $j_0, \ldots, j_{i-1}$ with $0 \leq j_b \leq 1$ for $b = 0, \ldots, i-1$ and an element $\gamma$ of $K$ for which

$$\theta_i = \alpha_0^{j_0} \theta_1^{j_1} \theta_2^{j_2} \cdots \theta_{i-1}^{j_{i-1}} \gamma^2.$$ (45)

But the order of the prime ideal $[\pi_i]$ on the left-hand side of (43) is 1 whereas the order on the right-hand side of (45) is even which is a contradiction. Thus (44) holds.

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

$$p^\nu/\delta \leq p.$$ (46)

Let us now determine $|\langle a_0, b_1, b_2, \ldots, b_k \rangle|$ in the case $\left(\frac{d}{p}\right) = -1$. By our earlier remarks the order of $\overline{\theta}_i$ is a divisor of $p + 1$ for $i = 2, \ldots, k$. Further by (27) since $N(\alpha/\beta) = 1$ we find that $N(\theta) = \pm 1$ and so $N(\theta^2) = 1$. By Hilbert’s Theorem 90, see eg. Theorem 14.35 of [9], $\theta^2 = \varrho/\varrho’$ where $\varrho$ and $\varrho’$ 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 $\left(\frac{d}{p}\right) = -1$, $[p]$ is a principal prime ideal of $\mathcal{O}_K$ and we note that $p$ does not divide $\varrho \varrho’$. It follows from Lemma 2 that the order of $\theta^2$ in $(\mathbb{Q}(\alpha/\beta))_p^\times$ is a divisor of $p + 1$ hence $\theta$ has order a divisor of $2(p + 1)$. Since $\alpha_0^4 = 1$ we conclude that

$$|\langle a_0, b_1, b_2, \ldots, b_k \rangle| \leq 2(p + 1)$$

and so

$$\delta = (p^2 - 1)/|\langle a_0, b_1, b_2, \ldots, b_k \rangle| \geq (p - 1)/2.$$ (47)
We now apply Lemma 5 noting, by (46) and (47), that
\[ p^f / \delta \leq 2p^2 / (p - 1). \]
Thus, by (32),
\[
\text{ord}_\wp (\alpha_1^m \theta_2^m \cdots \theta_k^m - 1) \leq c_8 (k + 1)^3 \log p \left( \frac{\pi_e p - 1}{p - 2} \right)^k 2^k p \left( \frac{k}{\log p} \right)^k (\log m) h(\alpha_1) h(\theta_2) \cdots h(\theta_k). \]

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 \( \theta_i \) over the integers since \( [\pi_i] \) is unramified. Either the
discriminant of \( Q(\alpha / \beta) \) 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 \( \pi_i \) by \( \pi_i \varepsilon^{u_i} \) for any
integer \( u_i \) and so without loss of generality we may suppose that \( p_i^{1/2} \leq |\pi'_i| \leq p_i^{1/2} \). Therefore
\[
h(\theta_i) \leq \left( \frac{1}{2} \right) \log p_i \varepsilon^2 = \left( \frac{1}{2} \right) \log p_i + \log \varepsilon \;
\text{for } d > 0
\]
and
\[
h(\theta_i) \leq \left( \frac{1}{2} \right) \log p_i \;
\text{for } d < 0.
\]
Let us put
\[
R = \begin{cases} 
\log \varepsilon & \text{for } d > 0 \\
0 & \text{for } d < 0.
\end{cases}
\]
Then
\[
h(\theta_i) \leq \left( \frac{1}{2} \right) \log p_i + R \quad \text{(49)}
\]
for \( i = 2, \ldots, k \). In a similar fashion we find that
\[
h(\theta_2 \cdots \theta_k) \leq \left( \frac{1}{2} \right) \log p_2 \cdots p_k + R, \quad \text{(50)}
\]
and so
\[
h(\alpha_1) \leq h(\theta) + \left( \frac{1}{2} \right) \log p_2 \cdots p_k + R. \quad \text{(51)}
\]
Put
\[ t_1 = \omega(2d p \alpha \beta). \]
Let \( q_i \) denote the \( i \)-th prime number which is representable as the norm of an
element of \( \mathcal{O}_K \). Note that
\[
p_k \leq q_{k+t_1}
\]
and thus
\[
\log p_2 + \cdots + \log p_k \leq (k - 1) \log q_{k+t_1}.
\]
Therefore by Lemma 4 for \( k > c_9 \),
\[
\log p_2 + \cdots + \log p_k \leq 1.0005 (k - 1) \log k \quad \text{(52)}
\]
and so, as for the proof of (38),
\[
\log p_2 \cdots \log p_k \leq (1.0005 \log k)^{k-1}.
\]
Accordingly, since \( p_k \geq k \), for \( k > c_{10} \)
\[
2^{k-1} h(\theta_2) \cdots h(\theta_k) \leq (\log p_2 + 2R) \cdots (\log p_k + 2R) \leq (1.001 \log k)^{k-1}. \quad \text{(53)}
\]
Furthermore as for the proof of (39) and (40) we find that from (51),
\[ h(\alpha_1) \leq c_{11} h(\theta) k \log k \] (54)
and, from (12), (28) and (33),
\[ h(\theta) \log m \leq 8 \log |\alpha| \log n. \] (55)
Thus by (43), (48), (51), (53), (54) and (55),
\[ \text{ord}_p((\alpha/\beta)^n - 1) < c_{12} k^4 \log p \left( 7e \left( \frac{p - 1}{p - 2} \right) 1.001 \frac{k \log k}{\log p} \right) p \log |\alpha| \log n. \] (56)
Therefore, by (31), for \( p > c_{13} \) we again obtain (41) and the result follows. \( \square \)

5. Proof of Theorem 1

Let \( c_1, c_2, \ldots \) denote positive numbers which are effectively computable in terms of \( \omega(\alpha \beta) \) and the discriminant of \( Q(\alpha/\beta) \). 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
\[ P(\Phi_n(\alpha, \beta)) \geq P(\Phi_n(\alpha_1, \beta_1)). \]
Therefore we may assume, without loss of generality, that \( (\alpha + \beta)^2 \) and \( \alpha \beta \) are coprime non-zero integers.

By Lemma 7 there exists \( c_1 \) such that if \( n \) exceeds \( c_1 \) then
\[ \log |\Phi_n(\alpha, \beta)| \geq \frac{\varphi(n)}{2} \log |\alpha|. \] (57)
On the other hand
\[ \Phi_n(\alpha, \beta) = \prod_{p|\Phi_n(\alpha, \beta)} p^{|\text{ord}_p\Phi_n(\alpha, \beta)|}. \] (58)
If \( p \) divides \( \Phi_n(\alpha, \beta) \) then, by (41), \( p \) does not divide \( \alpha \beta \) and so
\[ \text{ord}_p\Phi_n(\alpha, \beta) \leq \text{ord}_p((\alpha/\beta)^{n} - 1), \] (59)
where \( \varphi \) is a prime ideal of \( O_K \) lying above \( p \). By Lemma 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 8,
\[ \text{ord}_p((\alpha/\beta)^{n} - 1) < p \exp(-\log p/51.9 \log \log p) \log |\alpha| \log n. \] (60)
Put
\[ P_n = P(\Phi_n(\alpha, \beta)). \]
Then, by (58) and Lemma 1,
\[ \log |\Phi_n(\alpha, \beta)| \leq \log n + \sum_{p \leq P_n, p|n} \log p \text{ ord}_p\Phi_n(\alpha, \beta). \] (61)
Comparing (57) and (61) and using (59) and (60) we find that, for \( n > c_3 \),
\[ \varphi(n) \log |\alpha| < \sum_{p \leq P_n, p|n} \sum_{p|n} c_4 (\log p) \exp(-\log p/51.9 \log \log p) \log |\alpha| \log n \]
hence
\[ \frac{\varphi(n)}{\log n} < (\pi(P_n, n, 1) + \pi(P_n, n, -1))P_n \exp(- \log P_n / 51.95 \log \log P_n), \]
and, by Lemma 3,
\[ c_2 \frac{\varphi(n)}{\log n} < \frac{P_n^2}{\varphi(n) \log(P_n / n)} \exp(- \log P_n / 51.95 \log \log P_n). \]
Since \( \varphi(n) > c_6 n / \log \log n, \)
\[ P_n > n \exp(\log n / 104 \log \log n), \]
for \( n > c_7, \) as required.

6. Proof of Theorem 2

Since \( p \) does not divide \( ab \)
\[ \text{ord}_p (a^n - b^n) = \text{ord}_p ((a/g)^n - (b/g)^n) \]
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 \( n = 1, 2, \ldots \)
and let \( \ell = \ell(p) \) be the smallest positive integer for which \( p \) divides \( u_\ell. \) Certainly \( \ell \) divides \( p - 1. \) 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 \( \ell \) we see that \( (a, \ell) = \ell \) so that \( \ell \) divides \( n. \) In particular \( \ell \) divides \( p - 1. \) Furthermore, by (4), we see that
\[ \text{ord}_p u_\ell = \text{ord}_p \Phi_\ell(a, b). \]
If \( \ell \) divides \( n \) then, by Lemma 2 of [38],
\[ (u_n / u_\ell, u_\ell) \text{ divides } n / \ell, \]
and so
\[ \text{ord}_p u_{p-1} = \text{ord}_p u_\ell \]
(63)
Suppose that \( p \) divides \( \Phi_n(a, b). \) Then \( p \) divides \( u_n \) and so \( \ell \) 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 (62), since \( (t, p) = 1, \) that \( t = 1. \) Thus \( n = \ell p^k. \) For any positive integer \( m \)
\[ u_{mp} / u_m = p^{(m-1)p} + \left( \frac{p}{2} \right) b^{(m-2)p} u_m + \cdots + u_m^{p-1} \]
and if \( p \) is not 2 and \( p \) divides \( u_m \) then \( \text{ord}_p (u_{mp} / u_m) = 1. \) It then follows that if \( p \) is an odd prime then
\[ \text{ord}_p \Phi_{\ell p^k}(a, b) = 1 \quad \text{for } k = 1, 2, \ldots. \]
If $n$ is a positive integer not divisible by $\ell = \ell(p)$ then $|u_n|_p = 1$. On the other hand if $\ell$ divides $n$ and $p$ is odd then

$$|u_n|_p = |u\ell|_p \cdot |n/\ell|_p.$$  \hfill (64)

It now follows from (63) and (64) and the fact that $\ell \leq p - 1$ that if $p$ is an odd prime and $\ell$ divides $n$ then

$$|u_n|_p = |u_{p-1}|_p \cdot |n|_p.$$  \hfill (65)

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

$$\text{ord}_p(a^n - b^n) \leq \text{ord}_p(a^{p-1} - b^{p-1}) + \text{ord}_p n,$$

and our result now follows from (66) on taking $n = p - 1$ in Lemma 8.

REFERENCES

[1] M. Abramowitz and I.A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables, Dover Publications, New York, 1972.

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

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

[4] A.S. Bang, Taltheoretiske undersøgelser, Tidsskrift for Mat. 4 (1886), 70–78, 130–137.

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

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

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

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

[9] H. Cohn, A classical invitation to algebraic numbers and class fields, Springer-Verlag, New York, 1978.

[10] H. Cohn, Introduction to the construction of class fields, Cambridge studies in advanced mathematics 6, Cambridge University Press, Cambridge, 1985.

[11] L.E. Dickson, History of the theory of numbers, Vol. I, The Carnegie Institute of Washington, New York, 1952.

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

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

[14] P. Erdős, Some recent advances and current problems in number theory, Lectures on modern mathematics, Vol. III (ed. T.L. Saaty), Wiley, New York, 1965, 196–244.

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

[16] A. Fröhlich and M.J. Taylor, Algebraic number theory, Cambridge studies in advanced mathematics 27, Cambridge University Press, Cambridge, 1991.

[17] A.O. Gelfond, Transcendental and algebraic numbers, Dover Publications, New York, 1960.

[18] H. Halberstam and H.-E. Richert, Sieve methods, Academic Press, London, 1974.

[19] G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Oxford University Press, 5th ed, Oxford (1979).

[20] E. Hecke, Lectures on the theory of algebraic numbers, Graduate Texts in Mathematics 77, Springer-Verlag, New York, 1981.

[21] R. Juricevic, Lehmer numbers with at least 2 primitive divisors, Ph.D. thesis, University of Waterloo, 2007.

[22] D.H. Lehmer, An extended theory of Lucas’ functions, Ann. Math. 31 (1930), 419–448.
[23] J.C. Lagarias and A.M. Odlyzko, Effective versions of the Chebotarev Density Theorem, in *Algebraic Number Fields (L-functions and Galois properties)*, edited by A. Fröhlich, Academic Press, London, 1977, 409–464.

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

[25] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240, 289–321.

[26] Y. Matijasevic, Enumerable sets are diophantine (Russian), *Dokl. Akad. Nauk SSSR* **191** (1970), 279–282. Improved English translation: *Soviet Math. Doklady* **11** (1970), 354–357.

[27] L. Murata and C. Pomerance, On the largest prime factor of a Mersenne number, *CRM Proc. Lecture Notes* **36**, H. Kisilevsky and E.Z. Goren, editors, Amer. Math. Soc., Providence, R.I., 2004, 209–218.

[28] R. Murty and S. Wong, The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences, *Number Theory for the Millennium* III, edited by M.A. Bennett, B.C. Berndt, N. Boston, H.G. Diamond, A.J. Hildebrand and W. Philipp, A.K. Peters, Natick, MA, 2002, 43–54.

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

[30] A. Schinzel, On primitive prime factors of \(a^n - b^n\), *Proc. Cambridge Philos. Soc.* **58** (1962), 555–562.

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

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

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

[34] A. Schinzel, On primitive prime factors of Lehmer numbers, III, *Acta Arith.* **15** (1968), 49–69.

[35] A. Schinzel, Primitive divisors of the expression \(A^n - B^n\) in algebraic number fields, *J. reine angew. Math.* **268/269** (1974), 27–33.

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

[37] C.L. Stewart, The greatest prime factor of \(a^n - b^n\), *Acta Arith.* **26** (1975), 427–433.

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

[39] C.L. Stewart, Primitive divisors of Lucas and Lehmer numbers, *Transcendence theory: advances and applications* (eds. A. Baker and D.W. Masser), Academic Press, London, 1977, 79–92.

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

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

[42] P.M. Voutier, Primitive divisors of Lucas and Lehmer sequences, II, *J. Th. Nombres Bordeaux* **8** (1996), 251–274.

[43] P.M. Voutier, Primitive divisors of Lucas and Lehmer sequences, III, *Math. Proc. Camb. Phil. Soc.* **123** (1998), 407–419.

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

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

[46] T. Yamada, 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] K. Yu, \(P\)–adic logarithmic forms and group varieties I, *J. reine angew. Math.* **502** (1998), 29–92.

[48] K. Yu, New advances in \(p\)-adic theory of logarithmic forms, to appear.

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

C.L. Stewart, Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada, email: cstewart@uwaterloo.ca