ON DIVISORS OF FERMAT, FIBONACCI, LUCAS, AND LEHMER NUMBERS

By C. L. STEWART

[Received 22 May 1976]

1. Introduction

In [**32**] progress was made towards resolving the conjecture of Erdös (see [**12**, p. 218]) that $P(2^n-1)/n$ tends to infinity with n, where $P(m)$ denotes the greatest prime factor of m. The classical result that $P(a^n-b^n) \geqslant n+1$, when $n > 2$ and $a > b > 0$, follows from the work of several authors (see [**8**, Chapter XVI]), notably among them Bang [**4**], Zsigmondy [**37**], and Birkhoff and Vandiver [**5**]. In 1962 Schinzel [**23**] made the first advance on this result in more than seventy years by showing that $P(a^n-b^n) \geqslant 2n+1$ if ab is a square or twice a square; provided that one excludes the cases where $n = 4, 6, 12$ when $a = 2$ and $b = 1$. More recently, in [**32**], the author proved that

$$P(a^n-b^n)/n \to \infty \tag{1}$$

as n runs through a certain set of integers of density 1, in fact, those integers with less than $\kappa \log\log n$ distinct prime factors for any constant κ satisfying $0 < \kappa < 1/\log 2$. In the same paper it was proved that

$$P(a^p-b^p) > \tfrac{1}{2}p(\log p)^{\frac14}, \tag{2}$$

and also that

$$P(a^p+b^p) > p(\log p)^{\frac14}, \tag{3}$$

for all sufficiently large primes p, where the lower bound for these is effective.

Crucial to the proofs of (1), (2), and (3) were inequalities from the theory of linear forms in the logarithms of algebraic numbers. For the proof of (1) the then most recent result of Baker [**2**] in this field was required while for the proofs of (2) and (3) an older result of Baker [**1**] was used, which, while not as sharp as [**2**] in certain respects, was, unlike [**2**], totally explicit with regard to all the parameters involved. Since that time both Baker [**3**] and Shorey [**30**] have established results which possess the explicit character of [**1**] and which in addition are sufficiently sharp for our requirements. One of the purposes of this paper is to use the result of Baker [**3**] to strengthen inequalities (2) and (3) and further to determine a lower bound for how fast the expression in (1) tends to infinity with n.

A second purpose of this paper is to extend the results of [32] so as to include integer sequences like the Lucas and Lehmer numbers. We first indicate the results which have already been established in this context. Recall that *Lucas numbers* u_n and v_n satisfy

$$u_n = (\alpha^n - \beta^n)/(\alpha - \beta), \quad v_n = \alpha^n + \beta^n \quad (n > 0),$$

where α and β are distinct roots of a quadratic equation $x^2 - Px - Q = 0$ with relatively prime non-zero integer coefficients P and Q. In 1876 Lucas [19] announced several results which he had obtained concerning these numbers, earlier work having been done by Euler, Lagrange, Gauss, and Dirichlet, among others (see [8, Chapter XVII]), and in a long paper [20] published in 1878 he investigated their divisibility properties and gave evidence of their utility in a number of arithmetical settings; for example, in the rapid calculation of good rational approximations to quadratic irrationals (see [20, p. 225]) and also in the testing of Mersenne numbers for primality. For a clear rendering of Lucas' work in the latter instance the reader should consult papers of Lehmer [18] and Western [36].

Carmichael [7], in 1913, removed a number of errors from, and significantly clarified, the work of Lucas. It follows from Carmichael's study of the characteristic factors of u_n and v_n (see [7, Theorems XXI–XXVI]) that for α, β real and $n > 12$,

$$P(u_n) \geqslant n-1, \quad P(v_n) \geqslant 2n-1.$$

A *characteristic factor* of u_n, similarly of v_n, is a prime divisor of u_n which is not a factor of u_m for any $m < n$. All characteristic factors of u_n and v_n, which do not divide $(\alpha-\beta)^2$, are congruent to respectively $\pm 1 \pmod{n}$ and $\pm 1 \pmod{2n}$.

In 1930 Lehmer [17] generalized the results of Lucas on the divisibility properties of Lucas numbers to numbers u_n and v_n, with $n > 0$, satisfying

$$u_n \begin{cases} = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}, \\[2ex] = \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, \end{cases} \qquad v_n \begin{cases} = \dfrac{\alpha^n + \beta^n}{\alpha + \beta}, & \text{for } n \text{ odd}, \\[2ex] = \alpha^n + \beta^n, & \text{for } n \text{ even}, \end{cases}$$

where $(\alpha+\beta)^2$ and $\alpha\beta$ are relatively prime non-zero integers and α/β is not a root of unity. Note that $\alpha = \frac{1}{2}(\sqrt{r} + \sqrt{s})$ and $\beta = \frac{1}{2}(\sqrt{r} - \sqrt{s})$ where r and s are non-zero integers with $|r| \neq |s|$. The numbers u_n and v_n defined as above have come to be known as Lehmer numbers. It should be observed that Lucas numbers are also Lehmer numbers up to possible multiplication by a factor $\alpha + \beta$.

In 1955 Ward [**35**] investigated the intrinsic or characteristic divisors of Lehmer numbers as Carmichael had done for the Lucas numbers. These are defined as in the case of the Lucas numbers; furthermore, all intrinsic factors of u_n and of v_n, relatively prime to $(\alpha-\beta)^2(\alpha+\beta)^2$, are congruent to $\pm 1 \pmod{n}$ and $\pm 1 \pmod{2n}$ respectively. Ward proved that when α and β are real, u_n and v_n have intrinsic divisors for $n > 18$; and it may be deduced from Ward's work that for $n > 18$,

$$P(u_n) \geqslant n-1, \tag{4}$$

$$P(v_n) \geqslant 2n-1. \tag{5}$$

In fact, as Durst [**9**] pointed out, the restriction $n > 18$ in the preceding sentence may be replaced by $n > 12$.

In 1962 Schinzel [**24**] extended the work of Ward and Carmichael to include the case of Lehmer numbers with negative discriminants. In this case, where α and β are not real, he showed that both u_n and v_n have intrinsic divisors for n sufficiently large. Schinzel (see [**25**, p. 213]) defined primitive divisors of Lehmer numbers as intrinsic (prime) factors which do not divide $(\alpha-\beta)^2(\alpha+\beta)^2$, and in a postscript to [**24**] he noted that the Lehmer numbers u_n and v_n have primitive divisors, and as a consequence (4) and (5) hold, for all sufficiently large integers n.

Next Rotkiewicz [**22**], following Schinzel [**23**], considered the case of Lucas numbers with two primitive divisors (we remark that Rotkiewicz's definition of an intrinsic divisor can be shown to be equivalent to Schinzel's definition, which we shall adopt, of a primitive divisor), and then Schinzel, in a series of papers [**25, 26, 27, 28**], established conditions under which Lehmer numbers have two or more primitive factors. Schinzel deduced (see [**25**, Theorem 2] and the corrigenda with [**27**]), for real or complex α and β, that the right-hand side of (4) may be replaced by $n+1$ for n sufficiently large if $\pm\alpha\beta\max((\alpha-\beta)^2, (\alpha+\beta)^2)$ is a square or twice a square. Similarly, under the same hypotheses, (5) holds with $2n-1$ replaced by $2n+1$.

We shall strengthen the above results on the greatest prime factors of Lucas or Lehmer numbers in the case when α and β are real. We accomplish this by an analysis of the properties of the nth cyclotomic polynomial in α and β.

For any integer $n > 0$ and any pair of complex numbers α and β, we denote the nth *cyclotomic polynomial* in α and β by $\Phi_n(\alpha,\beta)$, that is,

$$\Phi_n(\alpha,\beta) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (\alpha-\zeta^j\beta), \tag{6}$$

where ζ is a primitive nth root of unity.

We also observe that $\Phi_n(\alpha,\beta)$ is an integer for $n > 2$ if $(\alpha+\beta)^2$ and $\alpha\beta$ are integers; for we note that both α^2 and β^2 are either rational integers or conjugate quadratic algebraic integers since both $(\alpha\beta)^2$ and $\alpha^2+\beta^2 = (\alpha+\beta)^2-2\alpha\beta$ are rational integers. But now, since Euler's phi-function $\varphi(n)$ is even for $n > 2$, we easily confirm that $\Phi_n(\alpha,\beta) = \Phi_n(\beta,\alpha)$ and thus further, that

$$\Phi_n(\alpha,\beta) = b_0 + \sum_{i=1}^{\frac{1}{2}\varphi(n)} b_i(\alpha^{2i}+\beta^{2i}),$$

where the b_i are integers since $\alpha\beta$ is an integer; whence $\varphi_n(\alpha,\beta)$ is a symmetric function of α^2 and β^2 and thus an integer.

We shall assume henceforth, unless we explicitly state otherwise, that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero relatively prime integers and further that α and β are distinct and real. Furthermore, we shall write

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

for $n > 2$.

Upon denoting the number of distinct prime factors of n by $\omega(n)$ and, further, the number of square-free divisors of n by $q(n) = 2^{\omega(n)}$ we may state

THEOREM 1. *For any κ with $0 < \kappa < 1/\log 2$ and any integer n (> 3) with at most $\kappa \log\log n$ distinct prime factors, we have*

$$P_n > C(\varphi(n)\log n)/q(n), \tag{7}$$

where C is a positive number which is effectively computable in terms of α, β, and κ only.

Since $\varphi(n) = n\prod_{p|n}(1-1/p)$ we clearly have

$$\varphi(n) \geqslant n\prod_{i=1}^{\omega(n)}(1-1/p_i),$$

where p_i denotes the ith prime number. Therefore from Mertens' theorem and the prime number theorem, we see that $\varphi(n) > cn/\log(1+\omega(n))$ for a positive absolute constant c. Thus, we may rewrite (7), in terms of n and $\omega(n)$ only, as

$$P_n > C_1(n\log n)/\{2^{\omega(n)}\log(1+\omega(n))\}, \tag{8}$$

or, on recalling that $\omega(n) < \kappa\log\log n$, wholly in terms of n as

$$P_n > C_2 n(\log n)^{\lambda}/\log\log\log n, \tag{9}$$

where $\lambda = 1-\kappa\log 2$ and where C_1 and C_2 are positive numbers which are effectively computable in terms of α, β, and κ only. The latter estimates are not as sharp as (7) insofar as, in determining a lower bound for $\varphi(n)$, the $\omega(n)$ distinct prime divisors of n were replaced by the first $\omega(n)$ primes.

In the case when α and β are integers Erdös and Shorey [**13**] have independently pointed out that the method of the author's paper [**32**] combined with [**30**] suffices to give a lower bound of the form (9); in fact the lower bound they obtain is slightly weaker than (9) as the $\log\log\log n$ term in the denominator on the right-hand side of (9) is replaced by $\log\log n$ in their work.

To illustrate the connection of the estimates (7), (8), and (9) for P_n with estimates for the greatest prime factor of Lucas or Lehmer numbers we use the equation

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha,\beta) \tag{10}$$

which follows immediately from (6). Upon noting that $\Phi_1(\alpha,\beta) = \alpha - \beta$ and also that $\Phi_2(\alpha,\beta) = \alpha+\beta$ we see that, for $n > 2$,

$$P(u_n) \geqslant P_n$$

for Lucas or Lehmer numbers u_n, and further that

$$P(a^n - b^n) \geqslant P_n$$

for rational integers a, b. We also have, on noting that $v_n = u_{2n}/u_n$ for Lucas or Lehmer numbers u_n and v_n, that, for $n > 1$,

$$P(v_n) \geqslant P_{2n}$$

and further that

$$P(a^n + b^n) \geqslant P_{2n}$$

for integers a, b.

Thus, on replacing P_n in (7), (8), or (9) by $P(a^n - b^n)$ we have an explicit bound for how fast the expression in (1) tends to infinity with n. In particular we see that (2) and (3) may now be improved to

$$P(a^p - b^p) > Cp \log p$$

and

$$P(a^p + b^p) > Cp \log p,$$

for $C = C(a,b) > 0$. Setting $a = 2$ and $b = 1$ in the former inequality gives us a lower bound for the greatest prime factor of any Mersenne number; the lower estimate in this special case has also been obtained independently in [**13**].

In addition, it clearly follows that (7), (8), and (9) hold with P_n replaced by $P(u_n)$ and P_{2n} replaced by $P(v_n)$ for any real Lucas or Lehmer numbers u_n and v_n; as a consequence we have, for integers n composed of at most k distinct primes, that $P(u_n) > Cn \log n$ and $P(v_n) > Cn \log n$ where $C = C(\alpha, \beta, k) > 0$.

We mention two more corollaries of Theorem 1 which are of some independent interest. The first of these concerns the Fermat numbers. It follows from Theorem 1 that

$$P(2^{2^n}+1) > Cn2^n \quad (n > 0)$$

for an effectively computable positive constant C.† The second concerns the Fibonacci numbers which are defined recursively by $u_1 = u_2 = 1$ and $u_n = u_{n-1}+u_{n-2}$. Now it is well known that the Fibonacci numbers are of the form

$$u_n = \{(\tfrac{1}{2}(1+\surd 5))^n - (\tfrac{1}{2}(1-\surd 5))^n\}/\surd 5,$$

and hence that they are real Lucas numbers. Thus Theorem 1 holds with P_n replaced by $P(u_n)$ and, in particular, we have for primes p

$$P(u_p) > Cp \log p,$$

where C is an effectively computable positive constant.

It is perhaps worthwhile to observe that the lower estimate for P_n given by (7) is almost certainly considerably weaker than the true value of P_n. Tables of Lucas and Lehmer numbers suggest that the greatest prime factor of $\Phi_n(\alpha, \beta)$ tends to infinity very rapidly with n. Furthermore, they indicate that $\Phi_n(\alpha, \beta)$ is only very rarely divisible by the square of a prime. The latter observation is related to the problem of the Fermat quotient when α and β are integers; see [**6**] for numerical work in this direction. From this observation one is led to conjecture that, for α, β real,

$$P_n > C(\varphi(n))^2 \tag{11}$$

for all integers n (> 2) where C is a positive effectively computable number. The conjecture certainly holds when $\Phi_n(\alpha, \beta)$ is square free, for then, from Lemma 6 of this paper, $P_n{}^T > \Phi_n$ where

$$T = \pi(P_n, n, 1) + \pi(P_n, n, -1) + 1;$$

and from the Brun–Titchmarsh inequality (see Lemma 10) and the estimate $\Phi_n > 2^{\frac{1}{2}\varphi(n)}$ (see [**35**, 4.1]), (11) follows. Quite likely even (11) is weak.

While we certainly cannot prove a result as sharp as (11) we can improve the lower estimate obtained in Theorem 1 for almost all integers n. We prove

THEOREM 2. *For almost all integers n*

$$P_n > n(\log n)^2/f(n)\log\log n \tag{12}$$

where $f(n)$ is any real-valued function for which $\lim_{n\to\infty} f(n) = \infty$.

† D. Kruyswijk has observed that the above estimate for the Fermat numbers may also be obtained by a more elementary argument.

As before, (12) holds with P_n replaced by the greatest prime factor of the Lucas or Lehmer numbers u_n or v_n and also with P_n replaced by $P(a^n - b^n)$ or $P(a^n + b^n)$ for integers a, b. The proof of Theorem 2 follows closely that of Theorem 1. A novel feature of the proof, however, is the use made of a lemma on consecutive divisors of integers, which follows from an old result of Erdös [**10**].

We note here that Erdös and Shorey [**13**] proved that

$$P(2^p - 1) > p(\log p)^2/(f(p)\log\log p \log\log\log p) \qquad (13)$$

for 'almost all' primes p. Their proof depends upon sieving techniques of Brun. It is readily verified that their argument, combined with the methods of this paper, allows one, in (13), to replace $2^p - 1$ by u_p, the pth Lucas or Lehmer number.

Theorems 1 and 2 may be used to strengthen a result of Schinzel concerning the greatest prime factors of the terms of certain binary recurrence sequences related to the Lehmer numbers. If $u_{n+1} = Pu_n - Qu_{n-1}$ where P and Q are rational integers, $PQ \neq 0$, $P^2 - 4Q \neq 0$, and $u_1^2 \neq u_0 u_2$, we have

$$u_n = \Omega\omega^n + \Omega'\omega'^n$$

where ω and ω' are solutions of $x^2 - Px + Q = 0$; here Ω and Ω' are computable in terms of ω, ω', u_0, and u_1. Schinzel proves (see [**29**, Theorem 8]) that if ω and ω' are real and, furthermore, ω/ω' and Ω/Ω' are multiplicatively dependent, then

$$P(u_n) > nv + u - 1$$

whenever $n > 0$ and $nv + u > 24$ where u and v are the integers with smallest absolute value such that

$$(\omega/\omega')^u = (-\Omega/\Omega')^v$$

with $v > 0$. Schinzel first shows that $P(u_n) > P_{(nv+u)/\sigma}$ where $\sigma = 1$ or 2. He then invokes the work of Ward [**35**] on intrinsic divisors of P_n to complete the proof. We point out that Theorems 1 and 2 may be applied in place of the work of Ward and thus, for example, (12) holds with P_n replaced by $P(u_n)$ for recurrence sequences u_n as above.

Further, we remark that analogues of Theorem 1 hold with α and β replaced by integer-valued functions $f(n)$ and $g(n)$. In fact, if for any positive integer n, $f(n) > g(n) > 0$, $f(n) < n^{\log n}$, and $f(n)/g(n) > c_0$ for $c_0 > 1$, then the statement of Theorem 1 applies with P_n replaced by $P(\Phi_n(f(n), g(n)))$ and C replaced by C', a positive number which is effectively computable in terms of κ and c_0 only. We shall not give the proof of this as it is essentially the same as that of Theorem 1; one simply makes explicit the dependence of C on α and β. As a consequence of the result quoted above, Theorem 1 holds with P_{2n} replaced by $P(\Phi_{2n}(n, 1))$ and C replaced by C', where $C' = C'(\kappa) > 0$, and thus applies to numbers of the form $n^n + 1$ (see Sierpinski [**31**]). Accordingly, if n is the product of at most k primes then

$$P(n^n+1) > Cn\log n$$

where C is a positive number which is effectively computable in terms of k only.

We shall next establish a lower estimate for P_n which applies when α and β are replaced by functions of n whose quotient tends to infinity with n rapidly, for example, exponentially rapidly. This lower estimate is sharper than that which one obtains by employing the argument used in the proof of Theorem 1.

Let $f(n)$, $g(n)$, and $l(n)$ be functions from the positive integers to the positive integers, and put $h(n) = f(n)^{l(n)}/g(n)$ and $P_n = P(\Phi_n(f(n)^{l(n)}, g(n)))$.

THEOREM 3. *If for any integer $n > 2$, $h(n) > 2^n$, and*

$$\max\{f(n), l(n)\} < n^{\log n},$$

then

$$P_n > C\varphi(n)\log\log h(n)$$

for an effectively computable positive constant C.

The two conditions in the statement of Theorem 3 are in no sense definitive and they certainly could be modified if an application so required. We mention two immediate consequences of Theorem 3. First, for integers $a > b > 1$, we have

$$P(a^{n^2}-b^n) > C\varphi(n)\log n$$

for $C = C(a,b) > 0$. Secondly, on recalling that $\varphi(n) > cn/\log\log n$ for some positive constant c, we find that

$$P(n^{n(n+1)}+(n+1)^n) > Cn\log n/\log\log n$$

for some effectively computable positive constant C. The first estimate follows on setting $f(n) = a$, $g(n) = b$, and $l(n) = n$ in Theorem 3; thus $h(n) = a^n/b$ which is greater than 2^n for n sufficiently large, since $a > 2$. Similarly, setting $f(n) = n$ and $g(n) = l(n) = n+1$, we see that the second estimate holds.

I would like to thank Professor A. Baker for his helpful suggestions concerning the presentation of this paper. I would also like to acknowledge the financial support which I received from the Canada Council while I was engaged on this research.

2. Preliminary lemmas on divisors of Lehmer numbers

The aim of this section is to give an account of the properties of divisors of Lehmer numbers relevant to this paper. We shall split the section into eight lemmas the first five of which are required solely for the proofs of the remaining three and are not, with the exception of Lemma 1, referred to subsequently. The latter three lemmas are employed in the proofs of Theorems 1, 2, and 3. Of these, Lemma 6 is the most important as it is essential to the proofs of all three main theorems. Lemmas 1–6 are not new insofar as they are consequences of combining the work of Lehmer [**17**] with the earlier work of Carmichael [**7**] and Lucas [**20**] on divisors of Lucas numbers. We feel it worthwhile to include short self-contained proofs for these lemmas since this obviates the necessity of labouring through [**7**, **17**, and **20**]. We note that the proofs given avoid the use of certain complicated identities favoured by Lucas and Lehmer. Lemma 7, which is crucial to the proof of Theorem 2, has not been explicitly stated before to my knowledge although it is certainly implicit in earlier work. Lastly, Lemma 8 is due to Ward [**35**] and is used for the proof of both Theorems 1 and 2.

We shall assume that $\alpha\beta$ and $(\alpha+\beta)^2$ are coprime non-zero rational integers and further that α/β is not a root of unity. The latter condition assures us that the expressions $\alpha+\beta$, and $\alpha^d-\beta^d$, for $d > 0$, which we intend to divide by in forthcoming arguments, are non-zero. We shall not require that α and β be real in Lemmas 1–7.

In the following lemmas $A_0, A_1, A_2, \ldots$ will denote algebraic integers. We prove

LEMMA 1. $(\alpha\beta, u_n) = (\alpha\beta, v_n) = 1$.

Proof. We may write

$$(\alpha+\beta)^{2n} = \alpha^{2n}+\beta^{2n}+\alpha\beta A_0 = v_{2n}+\alpha\beta A_0$$
$$= (\alpha^{2n+1}+\beta^{2n+1})/(\alpha+\beta)+\alpha\beta A_1 = v_{2n+1}+\alpha\beta A_1.$$

Thus $(\alpha\beta, v_n) = 1$ since, by assumption, $(\alpha\beta, (\alpha+\beta)^2) = 1$. Similarly we find, for n odd,

$$u_n = (\alpha^n-\beta^n)/(\alpha-\beta) = \alpha^{n-1}+\beta^{n-1}+\alpha\beta A_2 = v_{n-1}+\alpha\beta A_2,$$

and for n even,

$$u_n = (\alpha^n-\beta^n)/(\alpha-\beta)(\alpha+\beta) = (\alpha^{n-1}+\beta^{n-1})/(\alpha+\beta)+\alpha\beta A_3 = v_{n-1}+\alpha\beta A_3.$$

But $(\alpha\beta, v_n) = 1$, and therefore we have $(\alpha\beta, u_n) = 1$.

LEMMA 2. *If d divides n then $(u_n/u_d, u_d)$ divides n/d.*

Proof. If d divides n we have $\alpha^n = (\beta^d + (\alpha^d - \beta^d))^{n/d}$ and upon expanding the right-hand side we deduce that

$$(\alpha^n - \beta^n)/(\alpha^d - \beta^d) = (n/d)\beta^{n-d} + \binom{n/d}{2}\beta^{n-2d}(\alpha^d - \beta^d) + \ldots + (\alpha^d - \beta^d)^{(n/d)-1}. \quad (14)$$

On multiplying both sides of the above equation by α^{n-d} we find that, when $n-d$ is even,

$$\alpha^{n-d}u_n/u_d = (n/d)(\alpha\beta)^{n-d} + A_4 u_d,$$

and when $n-d$ is odd,

$$\alpha^{n-d}(\alpha+\beta)u_n/u_d = (n/d)(\alpha\beta)^{n-d} + A_5 u_d.$$

The lemma now follows by inspection of the above two equations since, by Lemma 1, $(\alpha\beta, u_n) = 1$.

Lemma 3. $(u_n, u_m) = u_{(n,m)}$ *for positive integers* m *and* n.

Proof. Given positive integers m and n we can certainly find positive integers r and s such that $rm - sn = (m, n)$. Let $rm = k$ and $sn = l$ so that $k - l = (k, l)$. We easily verify that

$$(\alpha^k - \beta^k)(\alpha^l + \beta^l) - (\alpha^l - \beta^l)(\alpha^k + \beta^k) = 2(\alpha\beta)^l(\alpha^{k-l} - \beta^{k-l}),$$

and since $k - l = (k, l)$ we have, for $k - l$ even,

$$u_k v_l - u_l v_k = 2(\alpha\beta)^l u_{k-l},$$

and for $k - l$ odd,

$$(\alpha+\beta)^2 u_k v_l - u_l v_k = 2(\alpha\beta)^l u_{k-l} \quad \text{for } l \text{ odd},$$

$$u_k v_l - (\alpha+\beta)^2 u_l v_k = 2(\alpha\beta)^l u_{k-l} \quad \text{for } k \text{ odd}.$$

If 2 does not divide (u_k, u_l) then from Lemma 1 and the above three equations, (u_k, u_l) divides u_{k-l}. Assume now that 2 divides both u_k and u_l. Since $u_{2k}/u_k = v_k$ we have, on setting $d = k$ and $n = 2k$ in the two equations below (14), that if k is even 2 divides v_k, while if k is odd 2 divides $(\alpha+\beta)^2 v_k$; and the same holds with k replaced by l. Thus from the above three equations we again find that (u_k, u_l) divides u_{k-l}. Now it follows from (10) that u_m divides u_k and that u_n divides u_l so therefore (u_m, u_n) must also divide (u_k, u_l); whence it divides $u_{k-l} = u_{(m,n)}$. But on once again recalling (10) we see that $u_{(m,n)}$ divides both u_m and u_n; thus the lemma holds.

From Lemma 1 we see that if a prime p divides $\alpha\beta$ it does not divide u_n for any integer n. We shall show, however, that each prime p which does not divide $\alpha\beta$ does in fact divide u_n for some integer n. We prove first

Lemma 4. *If* p *does not divide* $\alpha\beta(\alpha-\beta)^2(\alpha+\beta)^2$ *then* p *divides* $u_{p-1}u_{p+1}$.

Proof. We easily check that for primes $p > 2$

$$(\alpha-\beta)^2(\alpha+\beta)^2u_{p-1}u_{p+1} = \alpha^{2p}+\beta^{2p}-(\alpha^2+\beta^2)(\alpha\beta)^{p-1}.$$

By Fermat's theorem we then have

$$(\alpha-\beta)^2(\alpha+\beta)^2u_{p-1}u_{p+1} \equiv 0 \pmod{p},$$

and thus the lemma holds for $p > 2$.

For $p = 2$ we have $u_{p-1}u_{p+1} = u_3 = \alpha^2+\beta^2+\alpha\beta$, and if 2 does not divide $\alpha\beta u_3$ then it divides $\alpha^2+\beta^2+2\alpha\beta = (\alpha+\beta)^2$ and so the lemma holds. We note further that if 2 does not divide $\alpha\beta u_3$ then 2 must divide $u_4 = \alpha^2+\beta^2$.

LEMMA 5. *If p divides u_m $(m > 2)$ then p divides u_{mp}/u_m, and if $p > 2$ or if 4 divides u_m then in fact p $(\geqslant 2)$ divides u_{mp}/u_m to exactly the first power. If $p > 2$ divides $(\alpha-\beta)^2$ then p divides u_p, and if $p > 3$ then p exactly divides u_p. If p divides $(\alpha+\beta)^2$ then p divides u_{2p}, and if $p > 3$ then p exactly divides u_{2p}.*

Proof. From (14) we have, for any prime $p > 1$ and any positive integer m,

$$(\alpha^{mp}-\beta^{mp})/(\alpha^m-\beta^m) = p\beta^{m(p-1)}+\binom{p}{2}\beta^{m(p-2)}(\alpha^m-\beta^m)+\dots$$
$$+(\alpha^m-\beta^m)^{p-1}. \qquad (15)$$

We first prove the lemma for $p > 2$. From (15) we have

$$u_{mp}/u_m = pA_6+(\alpha^m-\beta^m)^{p-1} \quad (m \geqslant 1),$$

and since $A_7u_m = \alpha^m-\beta^m$ we see, for m > 2, that if p divides u_m then p divides u_{mp}/u_m. Setting $m = 1$ we find that if p divides $(\alpha-\beta)^2$ then p divides u_p; and, with $m = 2$, if p divides $(\alpha+\beta)^2$ then p divides u_{2p}.

We may also write, from (15),

$$\alpha^{m(p-1)}u_{mp}/u_m-p(\alpha^m-\beta^m)A_8-(\alpha^m-\beta^m)^{p-1}\alpha^{m(p-1)} = p(\alpha\beta)^{m(p-1)}$$

for $m \geqslant 1$. If p divides u_m for $m > 2$ then, since $\alpha^m-\beta^m = u_mA_9$, p^2 does not divide u_{mp}/u_m; for if it did we could write the left-hand side of the above equality as p^2A_{10}, where A_{10} is a non-zero integer, and thus p would divide $\alpha\beta$, contradicting Lemma 1. If $m = 1$ and $p > 3$ divides $(\alpha-\beta)^2$, then p^2 does not divide u_p; for otherwise, from the above equation, $p^2A_{11} = p(\alpha\beta)^{m(p-1)}$ which contradicts Lemma 1. Similarly, if $m = 2$ and $p > 3$ divides $(\alpha+\beta)^2$ then p divides u_{2p} to exactly the first power. We remark that if 3 divides $(\alpha-\beta)^2$ (respectively $(\alpha+\beta)^2$), it may, in fact, divide u_3 (respectively u_6) to a high power.

It remains only to prove the lemma for $p = 2$. In that case we have, from (15),

$$(\alpha^{2m}-\beta^{2m})/(\alpha^m-\beta^m) = 2\beta^m+(\alpha^m-\beta^m)$$

which is $(\alpha+\beta)u_{2m}/u_m$ for m odd and u_{2m}/u_m for m even. The lemma now follows as before if m is even or if m is odd and 2 does not divide $(\alpha+\beta)^2$. However, if 2 divides $(\alpha+\beta)^2$ then, as noted in the proof of Lemma 4, 2 must divide u_4 and so, from Lemma 3, 2 cannot divide u_m for m odd, whence the lemma holds.

If p does not divide $\alpha\beta$ then we may associate with it the smallest integer m for which p divides u_m. We see from Lemmas 4 and 5 that m exists. Now if p divides Φ_l then p divides u_l and from Lemma 3 and the minimality of m, $l = tmp^k$ for some $t \geqslant 1$, $(t,p) = 1$, and $k \geqslant 0$. In fact, $t = 1$, for otherwise p would divide both u_{tmp^k}/u_{mp^k} and u_{mp^k}, whence, from Lemma 2, p would divide t, contradicting the assumption $(t,p) = 1$. Thus if p divides Φ_l then $l = mp^k$.

If $p > 2$ is a prime which does not divide $(\alpha-\beta)^2(\alpha+\beta)^2\alpha\beta$ we have from Lemmas 3 and 4 that $m > 2$ divides either $p-1$ or $p+1$. Now since m is minimal, p divides Φ_m and, from Lemma 5 and the above paragraph, exactly divides Φ_{mp^k} $(k \geqslant 1)$. We note that for $k \geqslant 1$, $p = P(mp^k)$ since m divides $(p-1)(p+1)$ and hence is composed solely of primes less than p. Thus if p divides Φ_l then either $p = P(l)$ or $p \equiv \pm 1 \pmod{l}$.

If $p > 3$ divides $(\alpha-\beta)^2$, respectively $(\alpha+\beta)^2$, then, from Lemma 5, $m = p$, respectively $2p$, since $((\alpha+\beta)^2, (\alpha-\beta)^2)$ divides 2, and furthermore p exactly divides Φ_{p^k}, respectively Φ_{2p^k}, for $k \geqslant 1$. Similarly, if 3 divides $(\alpha-\beta)^2$ (respectively $(\alpha+\beta)^2$), then $m = 3$ (respectively 6), and 3 exactly divides Φ_{3^k} (respectively $\Phi_{2.3^k}$), for $k > 1$.

Lastly we consider $p = 2$. If 2 does not divide $\alpha\beta$ then, from the proof of Lemma 4, we see that either 2 divides $u_3 = \Phi_3$ or 2 divides $u_4 = \Phi_4$ and, from Lemma 5, 2 divides Φ_6 and exactly divides $\Phi_{3.2^k}$, for $k > 1$, in the former case, while 2 exactly divides Φ_{2^k}, for $k > 3$ (and, in fact, for $k = 3$ on noting that 2 divides both $(\alpha+\beta)^2$ and u_4), in the latter case.

We now have a rather accurate picture of the possible form of the prime decomposition of Φ_n which we shall summarize in the following manner.

Lemma 6. *If $n > 4$, and $n \neq 6, 12$, then $P(n/(3,n))$ divides Φ_n to at most the first power. All other prime factors of Φ_n are congruent to* $\pm 1 \pmod{n}$.

We note that if $n = 12$ the lemma holds with some divisor of 6 in place of $P(n/(3,n))$. From Lemma 6 we deduce

Lemma 7. *If $m > 2$ and $n > 4$ and $n \neq 6$ or 12 are distinct integers with $n > m$ then (Φ_n, Φ_m) divides $P(n/(3,n))$.*

Proof. If d divides (Φ_n, Φ_m) then clearly it divides (u_n, u_m) and, from Lemma 3, $u_{(n,m)}$. But now since $n > m$, Φ_n divides $u_n/u_{(n,m)}$ and from

Lemma 2 we see that d must divide n. The lemma now follows from Lemma 6.

Finally, we shall record a result, essentially due to Ward [**35**], on primitive divisors of Lehmer numbers with positive discriminant. Recall that a primitive divisor of the Lehmer number u_m is a prime which does not divide $(\alpha-\beta)^2(\alpha+\beta)^2u_3\dots u_{m-1}$. If α, β, defined as before, are real numbers we have

LEMMA 8. *u_n has a primitive divisor for $n > 12$.*

Proof. Ward [**35**] proved that $|\Phi_n| > n$ for $n > 12$ unless $\alpha = \pm\frac{1}{2}(1+\sqrt{5})$ and $\beta = \pm\frac{1}{2}(1-\sqrt{5})$ in which case $|\Phi_n| > n$ for $n > 30$. Now if $|\Phi_n| > n$ for $n > 12$ it plainly follows from Lemmas 6 and 7 that u_n has a divisor prime to $u_3\dots u_{n-1}$ and from the paragraphs preceding the statement of Lemma 6 we then see that u_n has, in fact, a primitive divisor. For the four Lehmer sequences related to the Fibonacci numbers we merely check that, for $n < 12 \leqslant 30$, u_n has a primitive divisor. This completes the proof.

Ward dealt with the very closely related problem of intrinsic divisors of Lehmer numbers. Unfortunately his preliminary analysis, §§ 2 and 3, is marred by a number of minor errors. These do not affect his subsequent work on estimates for Φ_n and hence do not affect the proof of Lemma 8. We note, however, that Theorem 1.2 of [**35**] is incorrect as stated; see Durst [**9**] for the requisite modifications.

3. Further preliminary lemmas

We shall now record a slightly modified version of the recent theorem of Baker mentioned in § 1. Let $\alpha_1, \dots, \alpha_n$ $(n > 1)$ be non-zero algebraic numbers with heights no greater than $A_1, \dots, A_n$ respectively $(A_i \geqslant 4)$, and let $b_1, \dots, b_n$ be rational integers with absolute values at most B $(\geqslant 4)$. Recall that the *height* of an algebraic number is defined as the maximum of the absolute values of the relatively prime integer coefficients in its minimal defining polynomial.

We assume that $\alpha_1, \dots, \alpha_n$ lie in a field of degree D over the rationals and write, for brevity,

$$\Lambda = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n \quad \text{and} \quad \Omega = \log A_1 \dots \log A_n.$$

We then have

LEMMA 9. *If $\Lambda \neq 0$ then*

$$\log|\Lambda| > -(nD)^{cn}\Omega(\log B)^2 \tag{16}$$

for an effectively computable positive constant c.

In fact Baker [3] established Lemma 9 with c explicitly computed and $(\log B)^2$ replaced by $\log B \log \Omega'$ where $\Omega' = \Omega/\log A_n$; this estimate is seen to be sharper than (16) if $A_n = \max_i A_i$ when it is taken in conjunction with the 'trivial' estimate $\log|\Lambda| > -nDB\log(3A_n)$. Shorey [30], on the other hand, obtained a weaker version of the lemma in which the right-hand side of the inequality was multiplied by $(\log\Omega + \log\log B)^{2n+7}$. However, neither of these variations in inequality (16) would have an effect on our results. What is important in the above estimates is the precise and explicit dependence obtained with respect to all the parameters involved and, in particular, with respect to the parameter n.

Next let $\pi(x, m, l)$ denote the number of primes not greater than x and equal to $l \pmod m$. We record the following version (see [15, Theorem 3.8]) of the Brun–Titchmarsh inequality:

LEMMA 10. *If* $1 \leqslant m < x$ *and* $(m, l) = 1$ *then*

$$\pi(x, m, l) < 3x/\varphi(m)\log(x/m).$$

While the constant 3 in the above inequality may be replaced by 2, see [21], such an improvement would only be significant if one was to calculate the numerical value of C in Theorem 1 for some α, β, and κ.

Finally, we require a result on the divisors of an integer n. Assume that the divisors are ordered according to size, and let $\varepsilon(n)$ be any real-valued function for which $\lim_{n\to\infty} \varepsilon(n) = 0$. We then have

LEMMA 11. *For almost all integers n, there exists an integer s, depending only on n, such that*

$$d_s/d_{s-1} > n^{\varepsilon(n)}. \tag{17}$$

We observe that Lemma 11 is best possible; for if the inequality (17) held with some positive constant ε in place of $\varepsilon(n)$ then, since $d_s/d_{s-1} \leqslant P(d_s) \leqslant P(n)$, almost all integers n would have a prime factor greater than n^ε. This is false, of course. In fact in 1925 Vinogradov [34] proved that the density of the set of integers n all of whose prime factors are less than n^ε exceeds $(u!(u+2)^u)^{-1}$ where $u = [\varepsilon^{-1}]$ and $u > u_0$; De Bruijn, Buchstab, and, most recently, Halberstam [14] have sharpened this lower estimate.

In 1936 Erdös [10] proved that: *if ε_a is an arbitrary function of a such that* $\lim_{a\to\infty} \varepsilon_a = 0$, *and if d_a denotes the density of the integers having a divisor between a and $a^{1+\varepsilon_a}$, then* $\lim_{a\to\infty} d_a = 0$; and in 1948 he remarked (see [11, p. 691]) that, by an argument similar to that used in [10], one could show that the number of integers not greater than n having a divisor in the interval $(n^{\frac{1}{2}-\varepsilon}, n^{\frac{1}{2}})$ is less than ηn where $\eta \to 0$ as $\varepsilon \to 0$. The latter statement implies Lemma 11. Accordingly we shall only give an outline of the proof of the lemma; the reader will be referred to [**10**] for the necessary details. We note, however, that our proof of Lemma 11 is significantly less complicated than that of the main theorem of [**10**].

Proof. Let ε be a small (<1) positive number and let $g, g_1, g_2, \ldots$ denote functions of ε satisfying $g_i(\varepsilon) \to 0$ as $\varepsilon \to 0$. We shall show that, for n sufficiently large depending on ε, the number of integers between n and $2n$ with a divisor between $n^{\frac{1}{2}}$ and $n^{\frac{1}{2}+\varepsilon}$ is less than $g(\varepsilon)n$. This will imply that, for n sufficiently large, all but $g(\varepsilon)n$ of the integers m between n and $2n$ have divisors d_s and d_{s-1} satisfying

$$d_s/d_{s-1} > n^{\varepsilon} > m^{\frac{1}{2}\varepsilon}$$

since we may set s equal to the index of the smallest divisor of m larger than $n^{\frac{1}{2}+\varepsilon}$. On letting $\varepsilon \to 0$ as $n \to \infty$ the lemma now follows easily.

We split the integers m between n and $2n$ having a divisor between $n^{\frac{1}{2}}$ and $n^{\frac{1}{2}+\varepsilon}$ into four disjoint sets. In the first set we put those integers divisible by an integer $A > n^{\varepsilon x}$ where A is composed solely of primes less than n^{ε} and where $x = \log(1/2\varepsilon)$. Arguing as in Lemma 1 of [**10**] with a replaced by n and ε_a by ε we find, for some positive constant c, that less than $cx^{-1}n$ integers are in the first set. We put in the second set those remaining integers which are divisible by at least $4x/3$ prime factors lying between n^{ε} and $n^{\frac{1}{2}+\varepsilon}$. It follows, from an argument of Turan (see either [**10**, Lemma 6] or [**33**]), that there are at most $g_1(\varepsilon)$ integers in this set.

The integers m which are left we split into two further sets, those divisible by integers l_m between $n^{\frac{1}{2}}$ and $n^{\frac{1}{2}+\varepsilon}$ with at most $2x/3$ distinct prime factors which lie between n^{ε} and $n^{\frac{1}{2}+\varepsilon}$, and those not so divisible. Plainly m is also divisible by m/l_m, an integer lying between $n^{\frac{1}{2}-\varepsilon}$ and $2n^{\frac{1}{2}}$. (Note that $2n^{\frac{1}{2}} < n^{\frac{1}{2}+\varepsilon}$ for n sufficiently large.) If m is in the latter set then m/l_m has at most $2x/3$ distinct prime factors between n^{ε} and $n^{\frac{1}{2}+\varepsilon}$, for otherwise m would be a member of the second set. But now for any integer m in the last two sets any divisor of either l_m or m/l_m which is composed solely of primes not greater than n^{ε} must be no larger than $n^{\varepsilon x}$ in size, since m is not a member of the first set. Thus all the integers m in the last two sets are divisible by integers B_i between $n^{\frac{1}{2}-\varepsilon(x+1)}$ and $n^{\frac{1}{2}+\varepsilon}$ with at most $2x/3$ distinct prime factors all of which lie between n^{ε} and $n^{\frac{1}{2}+\varepsilon}$. We may now prove, as in [**10**, Lemma 3], that $\sum_{i=1}^{\infty} 1/B_i < g_2(\varepsilon)$, and thus that there are at most $g_3(\varepsilon)n$ integers in the last two sets. Therefore the number of integers between n and $2n$ having a divisor between $n^{\frac{1}{2}}$ and $n^{\frac{1}{2}+\varepsilon}$ is less than $(g_1(\varepsilon)+g_3(\varepsilon)+cx^{-1})n$ and so less than $g(\varepsilon)n$, whence Lemma 11 follows, by our earlier remarks.

4. Proof of Theorem 1

Let $\alpha\beta$ and $(\alpha+\beta)^2$ be coprime non-zero integers with α, β distinct and real. We may assume, without loss of generality since $\Phi_n(\alpha,\beta)$ is symmetric in α and β for $n > 2$, that $\alpha > |\beta| > 0$. We shall further assume that n has at most $\kappa \operatorname{loglog} n$ distinct prime factors, where $0 < \kappa < 1/\log 2$, and that n exceeds a sufficiently large number which is effectively computable in terms of α, β ,and κ only.

Let $d_0 = 1$, and let $d_1, \ldots, d_t$ be all the divisors of n with $\mu(n/d_r) \neq 0$ ordered according to size. Then there exists an integer s, depending only on n, such that

$$d_s/d_{s-1} \geqslant \exp\{(\log n)/q(n)\} \tag{18}$$

$$\geqslant \exp\{(\log n)^{\lambda}\}, \tag{19}$$

where $\lambda = 1-\kappa \log 2$; note that $\lambda > 0$ since by hypothesis $\kappa < 1/\log 2$. In fact one can take s as the smallest integer not less than 1 such that $d_s \geqslant n^{s/t}$, which exists since $d_t = n$, and then clearly $d_s \geqslant n^{1/t} d_{s-1}$; but we have

$$t = q(n) \tag{20}$$

$$\leqslant 2^{\kappa \operatorname{loglog} n} = (\log n)^{\kappa \log 2}, \tag{21}$$

and so both (18) and (19) follow.

We now proceed, as in [**32**], to compare estimates for

$$R = \prod_{r=s}^{t} \{1-(\beta/\alpha)^{d_r}\}^{\mu(n/d_r)}.$$

First we have

$$\max\{R, R^{-1}\} \leqslant \prod_{r=s}^{t} (1-x^{d_r})^{-1},$$

where $x = |\beta/\alpha|$, and since, for d sufficiently large,

$$(1-x^d)^{-1} < 1+x^{d-1},$$

and, furthermore, by (19), $d_s \to \infty$ as $n \to \infty$, we see that the above product is at most

$$(1+x^{d_s-1})^t < 1+\sum_{l=1}^{t} (tx^{d_s-1})^l.$$

From (19) and (21) we clearly see that $tx^{d_s-1} < \frac{1}{2}$ for n sufficiently large, and thus, on recalling that $\kappa < 1/\log 2$, that the above sum does not exceed

$$2tx^{d_s-1} < x^{d_s} \log n.$$

Thus, since $\log(1+y) < y$ for $y > 0$, we obtain

$$|\log R| < |\beta/\alpha|^{d_s} \log n. \tag{22}$$

We prove now that $R \neq 1$ and hence that $|\log R| \neq 0$. If, for some pair of integers $n > 3$ and $s \geqslant 1$, $R = 1$ then from the definition of R it follows that

$$(\alpha^{a_1}-\beta^{a_1})\dots(\alpha^{a_j}-\beta^{a_j})\alpha^H = (\alpha^{a_{j+1}}-\beta^{a_{j+1}})\dots(\alpha^{a_k}-\beta^{a_k}) \tag{23}$$

with $k = t-s+1$, $H = \sum_{r=s}^{t} d_r\mu(n/d_r)$, and $a_1, \dots, a_j$, respectively $a_{j+1}, \dots, a_k$, given by those divisors d_r of n, where $s \leqslant r \leqslant t$, for which $\mu(n/d_r) = -1$, respectively $\mu(n/d_r) = 1$. We note that a_k may be taken to be n and that all the other a_i's are less than a_k. It now follows that the expression on the left-hand side of (23) may be written as the product of α^H, powers of $(\alpha-\beta)$ and $(\alpha+\beta)$, and some Lehmer numbers u_m with $m < n$. Similarly the expression on the right-hand side of (23) may be written as the product of u_n, Lehmer numbers u_m $(m < n)$, and powers of $(\alpha-\beta)$ and $(\alpha+\beta)$. On squaring the expressions on both sides of the equality, (23) becomes, for $H \geqslant 0$, an equation in integers only since $(\alpha-\beta)^2$ and $(\alpha+\beta)^2$ are integers. In fact $H = 0$ since, from Lemma 1, $(\alpha\beta, u_n) = 1$ and since also $(\alpha\beta, (\alpha-\beta)^2) = (\alpha\beta, (\alpha+\beta)^2) = 1$. From Lemma 8, however, we see that u_n has a primitive divisor for $n > 12$ and thus (23) cannot hold; as a consequence $R \neq 1$ for we may assume that $n > 12$.

We now employ Lemma 9 to derive a lower bound for $|\log R|$. We shall need the following identity

$$\Phi_n(\alpha,\beta) = \prod_{d|n} (\alpha^{n/d}-\beta^{n/d})^{\mu(d)} \tag{24}$$

which is easily verified from (10). From (24) we have

$$R = \alpha^{-H}\Phi_n(\alpha,\beta)\prod_{r=1}^{s-1}(\alpha^{d_r}-\beta^{d_r})^{-\mu(n/d_r)}, \tag{25}$$

where H is defined as above.

The product in (25) may be rewritten in the form

$$(\alpha-\beta)^K(\alpha^2-\beta^2)^L\prod_{r=1}^{s-1}((\alpha^{d_r}-\beta^{d_r})/(\alpha^{\delta}-\beta^{\delta}))^{-\mu(n/d_r)}, \tag{26}$$

where δ is 1 or 2 if d_r is respectively odd or even, and where

$$K = \sum_{\substack{r=1\\ 2\nmid d_r}}^{s-1} -\mu(n/d_r) \quad\text{and}\quad L = \sum_{\substack{r=1\\ 2|d_r}}^{s-1} -\mu(n/d_r).$$

The terms $(\alpha^{d_r}-\beta^{d_r})/(\alpha^{\delta}-\beta^{\delta})$ in (26) are the Lehmer numbers u_{d_r} and thus are integers which, since

$$(x^l-y^l)/(x-y) = x^{l-1}+x^{l-2}y+\dots+y^{l-1},$$

plainly do not exceed $d_r\alpha^{d_r-1} < (2\alpha)^{d_r}$ in absolute value. Furthermore, we note that

$$(\alpha-\beta)^K(\alpha^2-\beta^2)^L = (u/v)(\alpha-\beta)^{\gamma_1}(\alpha+\beta)^{\gamma_2},$$

where γ_1 and γ_2 are 0, 1, or -1, and where u, v are integers less than $(2\alpha^2)^{|K|+|L|}$ in absolute value. Thus the expression (26) is equal to $(a/b)(\alpha-\beta)^{\gamma_1}(\alpha+\beta)^{\gamma_2}$ where a, b are integers which, since $|K|+|L| < 2s$, are less than

$$(2\alpha)^{d_1+\dots+d_{s-1}+4s} < \alpha^{c_1 s d_{s-1}}$$

and so also, by (21), less than $\alpha^{c_2 \log n\, d_{s-1}}$ in absolute value; $c_1, c_2, \dots$ denote positive numbers which are effectively computable in terms of α, β, and κ. Therefore the height of the algebraic number represented by the product in (25) is bounded above by $\alpha^{c_3 \log n\, d_{s-1}}$.

We plainly have $|H| \leqslant \sum_{r=1}^{n} r \leqslant n^2$. Furthermore, by Lemma 6, we can write

$$\Phi_n(\alpha, \beta) = p_0 \prod_{j=1}^{k} p_j^{h_j}, \tag{27}$$

where $p_1, \dots, p_k$ are distinct primes congruent to $\pm 1 \pmod n$ and p_0 is 1 or $P(n/(3, n))$. Thus, on applying Lemma 9 with $\alpha_1, \dots, \alpha_n$ given respectively by $p_1, \dots, p_k$, p_0, α and the product in (25), and further recalling that $|\log R| \neq 0$, we obtain

$$|\log R| > \exp(-(nD)^{cn}\Omega(\log B)^2), \tag{28}$$

where $B = n^2$, $D = 4$, c is an effectively computable positive constant, and

$$\Omega = c_4 \log p_1 \dots \log p_k \log n \log A \log \alpha^{c_3 d_{s-1} \log n}$$

where $A = \max\{4, \text{height of } \alpha\}$.

But now we can assume that $p_1, \dots, p_k$ are all less than n^2, for otherwise the theorem is certainly valid and thus

$$\Omega \leqslant c_5 2^k (\log n)^{k+2} d_{s-1}.$$

Therefore, on combining (28) and (22), we find that

$$d_s \log|\alpha/\beta| - \log\log n < (k \log n)^{c_6 k} d_{s-1}. \tag{29}$$

This, together with (18), gives

$$(\log n)/q(n) < c_7 k(\log k + \log\log n),$$

and thus we have

$$k > c_8 (\log n)/q(n) \log\log n. \tag{30}$$

It follows from Lemma 6 that at least half of the primes $p_1, \dots, p_k$ are congruent to one of either $+1$ or $-1 \pmod n$; and we may assume, as it makes no difference to the rest of the argument, that at least half are congruent to $-1 \pmod n$. Let P denote the maximum of the p_i's congruent to $-1 \pmod n$. We then have from (30) and from Lemma 10, on setting $l = -1$, $m = n$, and $\pi(x, m, l) = [\frac{1}{2}k]$, that

$$c_9 (\varphi(n) \log n)/q(n) \log\log n < x/\log(x/n) \tag{31}$$

for some integer $x \leqslant P$. Now since $\varphi(n) > c_{10}n/\log\log n$, and further since, from (21), $(\log n)/q(n) > (\log n)^{\lambda}$, for $\lambda > 0$, we conclude that

$$x > c_{11}n(\log n)^{\lambda}/(\log\log n)^2.$$

Therefore $\log(x/n) > c_{12}\log\log n$ and it follows from (31) that

$$x > c_{13}(\varphi(n)\log n)/q(n),$$

whence the theorem holds since $P_n \geqslant P \geqslant x$.

5. Proof of Theorem 2

The proof of Theorem 2 follows closely that of Theorem 1. Accordingly we shall refer the reader to the proof of Theorem 1, when it is appropriate, rather than repeat the same arguments.

We assume that for some function $f(n)$, as in the statement of the theorem, and some positive constant δ, there exist arbitrarily large integers n with at least δn integers m, between n and $2n$, satisfying

$$P_m < m(\log m)^2/f(m)\log\log m, \tag{32}$$

for if there exists no such pair δ, f, then the theorem plainly holds. We further assume, without loss of generality, that $f(n)$ is an increasing function.

Now, as before, let $d_0 = 1$ and, for any integer n, let $d_1, \ldots, d_t$ be all the divisors of n with $\mu(n/d_r) \neq 0$ ordered according to size. From Lemma 11 we observe that there exists an integer s, depending only on n, such that

$$d_s/d_{s-1} > \exp\{(\log n)/(f(n))^{\frac{1}{2}}\}, \tag{33}$$

and also, since plainly we may assume that $(f(n))^{\frac{1}{2}} < \log\log n$,

$$d_s/d_{s-1} > \exp\{(\log n)/\log\log n\} \tag{34}$$

for almost all integers n. Furthermore, almost all integers n have $(1+o(1))\log\log n$ distinct prime factors (see [**16**, p. 356]) and thus have

$$\begin{aligned} t &\leqslant 2^{(1+o(1))\log\log n} \\ &< (\log n)^{\frac{3}{4}}. \end{aligned} \tag{35}$$

Thus there exist arbitrarily large integers n with at least $\frac{1}{2}\delta n$ integers m between n and $2n$ satisfying (32), (33), (34), and (35). Given such an integer n, we may estimate the number of distinct prime factors of Φ_m for each of the $\frac{1}{2}\delta n$ integers m between n and $2n$, as in the proof of Theorem 1, with (34) and (35) in place of (19) and (21) respectively. We argue as before (note that the p_i are less than P_m and thus, from (32), are less than n^2, as was assumed in the proof of Theorem 1) until we reach (29) at which point we have

$$d_s/d_{s-1} < (k\log n)^{c_{14}k}. \tag{36}$$

Since $f(n)$ is strictly increasing we conclude, from (33) and (36), that

$$(\log n)/(f(2n))^{\frac{1}{2}} < c_{15}k(\log k + \log\log n).$$

Further, since we may assume that $(f(n))^{\frac{1}{2}} < \log\log n$, it plainly follows that

$$(\log n)/(f(n))^{\frac{1}{2}} \log\log n < k$$

for n sufficiently large.

Thus we may find arbitrarily large integers n with at least $\frac{1}{2}\delta n$ integers m between n and $2n$ satisfying (32) and for which the number of distinct prime factors of Φ_m exceeds $(\log n)/(f(n))^{\frac{1}{2}} \log\log n$. Therefore, from Lemma 7 and (32), there are $(\delta n \log n)/2(f(n))^{\frac{1}{2}} \log\log n - \frac{1}{2}\delta n$ distinct prime numbers less than $4n(\log n)^2/f(n)\log\log n$ for infinitely many integers n. This contradicts the prime number theorem for n sufficiently large, however, and the theorem now follows by our earlier remarks.

6. Proof of Theorem 3

We shall assume throughout that n exceeds a sufficiently large number c_1; here $c_1, c_2, \ldots$ denote effectively computable positive numbers.

We now proceed to compare estimates for

$$\begin{aligned} R &= \Phi_n((f(n))^{l(n)}, g(n))/(f(n))^{l(n)\varphi(n)} \\ &= 1 - \mu(n)/h(n) + t_2/(h(n))^2 + \ldots + t_{\varphi(n)}/(h(n))^{\varphi(n)} \end{aligned}$$

where the t_i's are the coefficients of the cyclotomic polynomial. The t_i's are the values of the elementary symmetric functions on the primitive nth roots of unity and as such are integers satisfying $|t_i| < \binom{n}{i} \leqslant n^i$.

But now, since $(1-x) \leqslant (1+x)^{-1}$ for $x \geqslant 0$, we have

$$\min\{R, R^{-1}\} \geqslant 1 - \{(1 + (n^2/h(n)) + \ldots + (n^2/h(n))^{\varphi(n)-1})/h(n)\}$$

and, since $(n^2/h(n)) < \frac{1}{2}$ for n sufficiently large, this is at least $1 - 2/h(n)$. Thus, on recalling that $|\log(1-y)| < 2y$ for $0 < y < \frac{1}{2}$, we find that

$$|\log R| < 4(h(n))^{-1}. \tag{37}$$

We now prove that $R \neq 1$ and hence that $|\log R| > 0$. We observe that a root of the monic polynomial $\Phi_n(1, x) - 1$ $(n > 2)$ is an algebraic integer. But now $R = \Phi_n(1, (h(n))^{-1})$, and thus if $R = 1$ then $(h(n))^{-1}$ is a root of $\Phi_n(1, x) - 1$. This gives a contradiction, however, since $(h(n))^{-1}$ is a rational number between 0 and 1 and thus is not an algebraic integer.

We now employ Lemma 9 to give a lower bound for $|\log R|$ in terms of the number of distinct prime factors of $\Phi_n((f(n))^{l(n)}, g(n))$. We observe that we may write

$$R = p_0 \prod_{j=1}^{k} p_j^{h_j} (f(n))^{-\varphi(n)l(n)}$$

where, from Lemma 6, $p_0 = 1$ or $P(n/(3,n))$, $p_1, \ldots, p_k$ are distinct primes congruent to $\pm 1 \pmod{n}$; in fact, we may assume they are congruent to $+1 \pmod{n}$ (see [5]) and $h_1, \ldots, h_k$ are positive integers. Thus, on applying Lemma 9 with $D = 1$, $n = k+2$, and with $\alpha_1, \ldots, \alpha_n$ given respectively by $p_1, \ldots, p_k$, p_0, and $f(n)$, we find, since $|\log R| \neq 0$, that

$$|\log R| > \exp(-n^{cn}\Omega(\log B)^2), \tag{38}$$

where $B = \varphi(n)l(n)\log f(n)$, c is an effectively computable positive number, and

$$\Omega = \log p_1 \ldots \log p_k \log n \log(4f(n)).$$

We assume, as before, that the p_i's are all less than n^2; for otherwise the theorem plainly holds since $h(n) \leqslant f(n)^{l(n)}$ and $\max\{f(n), l(n)\} < n^{\log n}$, whence $\log\log h(n) < n$ for n sufficiently large. Therefore

$$\Omega \leqslant c_2 2^k (\log n)^{k+3}.$$

Furthermore, since $l(n) \leqslant n^{\log n}$, we have $B \leqslant c_3 n^{3+\log n}$. Accordingly, on combining (37) and (38) and taking logarithms, we find that

$$\log h(n) < (k \log n)^{c_4 k}.$$

This implies that

$$c_5 k > \min\{\log\log h(n)/\log\log n,\ \log\log h(n)/\log\log\log h(n)\}$$

which, because $h(n) > 2^n$, is greater than

$$c_6 \log\log h(n)/\log\log\log h(n).$$

On setting $m = n$, $l = 1$, and $\pi(x, m, l) = k$ in Lemma 10, we find that

$$c_7 \varphi(n) \log\log h(n)/\log\log\log h(n) < x/\log(x/n) \tag{39}$$

for some integer $x \leqslant P_n$. Now since the k distinct primes p_i are congruent to $1 \pmod{n}$, we have

$$x > c_8 n \log\log h(n)/(\log\log\log h(n))^2,$$

whence, from (39),

$$x > c_9 \varphi(n) \log\log h(n).$$

This completes the proof of the theorem since $x \leqslant P_n$.

REFERENCES

1. A. Baker, 'Linear forms in the logarithms of algebraic numbers IV', *Mathematika* 15 (1968) 204–16.
2. —— 'A sharpening of the bounds for linear forms in logarithms III', *Acta Arith.* 27 (1975) 247–52.
3. —— 'The theory of linear forms in logarithms', *Transcendence theory: advances and applications* (ed. A. Baker and D. Masser, Academic Press, London, 1977).
4. A. S. Bang, 'Taltheoretiske undersøgelser', *Tidsskrift for Mat.* (5) 4 (1886) 70–80, 130–37.

5. G. D. Birkhoff and H. S. Vandiver, 'On the integral divisors of $a^n - b^n$', *Ann. of Math.* (2) 5 (1904) 173–80.

6. J. Brillhart, J. Tonascia, and P. Weinberger, 'On the Fermat quotient', *Computers in number theory* (ed. A. O. L. Atkin and B. J. Birch, Academic Press, London, 1971), pp. 213–22.

7. R. D. Carmichael, 'On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$', *Ann. of Math.* (2) 15 (1913) 30–70.

8. L. E. Dickson, *History of the theory of numbers*, Vol. I (The Carnegie Institute of Washington, New York, 1952).

9. L. K. Durst, 'Exceptional real Lehmer sequences', *Pacific J. Math.* 9 (1959) 437–41.

10. P. Erdös, 'A generalization of a theorem of Besicovitch', *J. London Math. Soc.* 11 (1936) 92–98.

11. —— 'On the density of some sequences of integers', *Bull. Amer. Math. Soc.* (2) 54 (1948) 685–92.

12. —— 'Some recent advances and current problems in number theory', *Lectures on modern mathematics*, Vol. III (ed. T. L. Saaty, Wiley, New York, 1965), pp. 196–244.

13. —— and T. N. Shorey, 'On the greatest prime factor of $2^p - 1$ for a prime p and other expressions', *Acta Arith.*, 30 (1976) 257–65.

14. H. Halberstam, 'On integers all of whose prime factors are small', *Proc. London Math. Soc.* (3) 21 (1970) 102–7.

15. —— and H.-E. Richert, *Sieve methods* (Academic Press, London, 1974).

16. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th edn (Oxford University Press, 1960).

17. D. H. Lehmer, 'An extended theory of Lucas' functions', *Ann. of Math.* (2) 31 (1930) 419–48.

18. —— 'On Lucas's test for the primality of Mersenne's numbers', *J. London Math. Soc.* 10 (1935) 162–65.

19. E. Lucas, 'Sur les rapports qui existent entre la théorie des nombres et le calcul intégral', *C. R. Acad. Sci. Paris*, 82 (1876) 1303–5.

20. —— 'Théorie des fonctions numériques simplement périodiques', *Amer. J. Math.* 1 (1878) 184–240, 289–321.

21. H. L. Montgomery and R. C. Vaughan, 'The large sieve', *Mathematika* 20 (1973) 119–34.

22. A. Rotkiewicz, 'On Lucas numbers with two intrinsic prime divisors', *Bull. Acad. Polon. Sci. Sér. Math. Astr. Phys.* 10 (1962) 229–32.

23. A. Schinzel, 'On primitive prime factors of $a^n - b^n$', *Proc. Cambridge Philos. Soc.* 58 (1962) 555–62.

24. —— 'The intrinsic divisors of Lehmer numbers in the case of negative discriminant', *Ark. Mat.* 4 (1962) 413–16.

25. —— 'On primitive prime factors of Lehmer numbers I', *Acta Arith.* 8 (1963) 213–23.

26. —— 'On primitive prime factors of Lehmer numbers II', ibid. 8 (1963) 251–57.

27. —— 'On primitive prime factors of Lehmer numbers III', ibid. 15 (1968) 49–69.

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

29. —— 'On two theorems of Gelfond and some of their applications', *Acta Arith.* 13 (1967) 177–236.

30. T. N. Shorey, 'On linear forms in the logarithms of algebraic numbers', ibid. 30 (1976) 27–42.

31. W. Sierpiński, 'Sur les nombres premiers de la forme $n^n + 1$', *Enseignement Math.* (2) 4 (1958) 211–12.

32. C. L. Stewart, 'The greatest prime factor of $a^n - b^n$', *Acta Arith.* 26 (1975) 427–33.

33. P. Turán, 'On a theorem of Hardy and Ramanujan', *J. London Math. Soc.* 9 (1934) 274–76.

34. I. M. Vinogradov, 'On bounds for least nth power non-residues', *Izv. Akad. Nauk. SSSR.* 20 (1926) 47–58.

35. M. Ward, 'The intrinsic divisors of Lehmer numbers', *Ann. of Math.* (2) 62 (1955) 230–36.

36. A. E. Western, 'On Lucas's and Pepin's tests for the primeness of Mersenne's numbers', *J. London Math. Soc.* 7 (1932) 130–37.

37. K. Zsigmondy, 'Zur Theorie der Potenzreste', *Monatsh. Math.* 3 (1892) 265–84.

Trinity College
Cambridge

Present address:
Institut des Hautes Études Scientifiques
91440 Bures-sur-Yvette, France