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

T. N. SHOREY AND C. L. STEWART

1. *Introduction*

Let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero relatively prime integers and α/β is not a root of unity. For any positive integer n we denote the n-th cyclotomic polynomial in α and β by $\Phi_n(\alpha, \beta)$, that is,

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

where ζ is a primitive n-th root of unity. Observe that for n at least 3, $\Phi_n(\alpha, \beta)$ is a rational integer (see [**5**; p. 428]). For any integer n let $P(n)$ denote the greatest prime factor of n, with the convention that $P(0) = P(\pm 1) = 1$, and for n at least 3 put $P_n = P(\Phi_n(\alpha, \beta))$. Further for any positive integer n denote the number of distinct prime divisors of n by $\omega(n)$ and put $q(n) = 2^{\omega(n)}$, the number of square-free divisors of n. Lastly recall that $\phi(n)$ is the number of positive integers less than or equal to n and coprime to n. We are now able to state our first theorem.

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

$$P_n > C(\phi(n)\log n)/q(n), \tag{2}$$

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

For $n > 12$, all the prime factors of $\Phi_n(\alpha, \beta)$ are congruent to $\pm 1 (\operatorname{mod} n)$ with the possible exception of $P(n/(3, n))$ which may divide $\Phi_n(\alpha, \beta)$ but to the first power only (see [**5**, Lemma 6]). Schinzel [**3**] proved that $|\Phi_n(\alpha, \beta)|$ is larger than n and as a consequence that

$$P_n \geqslant n-1, \tag{3}$$

for n sufficiently large; by a result of Stewart [**6**] it suffices to take n larger than $e^{452} \cdot 4^{67}$. We remark that estimate (2) is more precise than estimate (3) except for a set of integers n of asymptotic density zero since almost all integers n have $(1+o(1))\operatorname{loglog} n$ distinct prime factors. In particular if n is composed of at most k distinct prime factors then

$$P_n > C_1 n \log n,$$

where C_1 is a positive number which is computable in terms of α, β and k only.

Received 14 August, 1979.

The research of the second author was supported in part by a University of Waterloo Research Grant and Natural Sciences and Engineering Research Council Grant A3528.

[J. LONDON MATH. SOC. (2), 23 (1981), 17–23]

We are able to improve upon estimates (2) and (3) if we ask for a lower bound for P_n which applies for all integers n except perhaps for those in some unspecified set of asymptotic density zero.

THEOREM 2. *For "almost all" integers n,*

$$P_n > n(\log n)^2/f(n)\log\log n\,, \tag{4}$$

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

Stewart [5] proved both Theorems 1 and 2 in the case where α and β are real numbers; in fact these results will be used for the proofs of the two theorems. For a survey of earlier results obtained in the direction of Theorems 1 and 2 we refer the reader to [5].

The above theorems derive much of their interest from the link between $\Phi_n(\alpha, \beta)$ and the Lucas and Lehmer numbers. These numbers arise in a multitude of arithmetical settings. The 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 $\alpha+\beta$ and $\alpha\beta$ are relatively prime non-zero integers and α/β is not a root of unity, while the Lehmer numbers u_n and v_n satisfy

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

where $(\alpha+\beta)^2$ and $\alpha\beta$ are relatively prime non-zero integers and α/β is not a root of unity. The connexion between the estimates (2), (3) and (4) for P_n with estimates for the greatest prime factor of Lucas or Lehmer numbers is given by the equation

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta)\,, \tag{5}$$

which follows directly from (1). Upon noting that $\Phi_1(\alpha, \beta) = \alpha - \beta$ and $\Phi_2(\alpha, \beta) = \alpha + \beta$ we see that for $n > 2$, $P(u_n) \geqslant P_n$, for Lucas or Lehmer numbers u_n. Further, on observing that $v_n = u_{2n}/u_n$ for Lucas or Lehmer numbers u_n and v_n we have that for n at least 2, $P(v_n) \geqslant P_{2n}$.

When α and β are rational integers we are able to show that the number C which occurs in the statement of Theorem 1 and which can be computed in terms of α, β and κ can in fact be determined in terms of κ and the greatest prime factor of $\alpha\beta$ only.

THEOREM 3. *Let α and β be non-zero integers with $|\alpha| \neq |\beta|$. Then for any κ with $0 < \kappa < 1/\log 2$ and any integers $n(>3)$, with at most $\kappa\log\log n$ distinct prime factors we have*

$$P_n > C_2(\phi(n)\log n)/q(n)\,,$$

where C_2 is a positive number which is effectively computable in terms of $P(\alpha\beta)$ and κ only.

In particular, if a and b are distinct positive integers and p denotes a prime number then, from (5),

$$P(a^p - b^p) > C_4 p \log p,$$

and

$$P(a^p + b^p) > C_5 p \log p,$$

where C_4 and C_5 are positive numbers which are effectively computable in terms of $P(ab)$ only.

The above three theorems are obtained by combining a p-adic generalization of Baker's theorem on linear forms in the logarithms of algebraic numbers with the methods of [4] and [5]. We shall use the following p-adic estimate due to van der Poorten [2] in our proofs.

LEMMA 1. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be non-zero algebraic numbers and let K be their splitting field over $\mathbb{Q}$, the rational numbers. Put $D = [K : \mathbb{Q}]$ and denote by $A_1, \ldots, A_n$ upper bounds for the heights of $\alpha_1, \ldots, \alpha_n$ respectively, where we assume that $A_j \geqslant 2$ for $1 \leqslant j \leqslant n$. Write*

$$\Omega = \prod_{j=1}^{n} \log A_j .$$

Let $\mathfrak{p}$ be a prime ideal of K lying above the rational prime p. Then there exists an effectively computable positive constant C_3 such that the inequalities

$$\infty > \operatorname{ord}_{\mathfrak{p}}(\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1) > (2nD)^{C_3 n} \frac{p^D}{\log p} \Omega (\log B)^2$$

have no solution in rational integers $b_1, \ldots, b_n$ with absolute values at most B for $B \geqslant 2$.

2. *Proof of Theorem* 1

Note 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 $|r| \neq |s|$. Put $K = \mathbb{Q}(\alpha, \beta)$. As mentioned in §1, Stewart [5] proved Theorem 1 when α and β are real numbers. In view of this result we can assume that r and s are of opposite sign. If both α and β are units in K then α/β is a unit in the imaginary quadratic field $\mathbb{Q}(\sqrt{rs})$ and hence α/β is a root of unity. Thus we can assume that either α or β is not a unit in K. It is no loss of generality to assume that α is not a unit in K. We shall assume also that n exceeds a sufficiently large number c_1, where $c_1, c_2, \ldots$ are positive numbers which are effectively computable in terms of α, β and κ only.

Let $d_0 = 1$ and let $d_1 < d_2 < \ldots < d_t$ be all the positive divisors of n with $\mu(n/d_r) \neq 0$. Then there exists a positive integer s, depending on n, such that

$$d_s/d_{s-1} \geqslant n^{1/t} = \exp\left((\log n)/q(n)\right) \geqslant \exp\left((\log n)^{\frac{1}{2}}\right), \tag{6}$$

where $\lambda = 1 - \kappa \log 2$; note that $\lambda > 0$ since by hypothesis $\kappa < 1/\log 2$. From (5) we have

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

Put

$$A = \prod_{r=1}^{s-1} (\alpha^{d_r} - \beta^{d_r})^{\mu(n/d_r)}, \quad M = \sum_{r=s}^{t} \mu(n/d_r) \quad \text{and} \quad N = \sum_{r=s}^{t} d_r \mu(n/d_r).$$

Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ all the prime ideals in K which divide the ideal generated by α. Since $((\alpha+\beta)^2, \alpha\beta) = 1$ these ideals are coprime to the ideal generated by β. It is now straightforward to check that

$$|\Phi_n(\alpha, \beta) A^{-1} - (-1)^M \beta^N|_{\mathfrak{p}_j} \leqslant |\alpha|_{\mathfrak{p}_j}^{d_s}, \tag{7}$$

for $1 \leqslant j \leqslant l$. Further, for $n > 12$,

$$\Phi_n(\alpha, \beta) = p_0 \prod_{i=1}^{k} p_i^{h_i},$$

where $p_1, \ldots, p_k$ are distinct primes congruent to $\pm 1 \pmod n$ and $\pm p_0$ is 1 or the greatest prime factor of $n/(3, n)$ (see [**5**; Lemma 6]). Therefore, from (7), we have

$$|(-1)^M p_0 p_1^{h_1} \ldots p_k^{h_k} \beta^{-N} A^{-1} - 1|_{\mathfrak{p}_j} \leqslant |\alpha|_{\mathfrak{p}_j}^{d_s}, \tag{8}$$

for $1 \leqslant j \leqslant l$.

Schinzel [**3**] proved, see also [**6**], that for n larger than some absolute constant $\Phi_n(\alpha, \beta)$ is divisible by a prime ideal in K which does not divide the ideal generated by $(\alpha-\beta)(\alpha^2-\beta^2)\ldots(\alpha^{n-1}-\beta^{n-1})$. This ideal is also coprime to the ideal generated by β since $((\alpha+\beta)^2, \alpha\beta) = 1$ and therefore

$$\Phi_n(\alpha, \beta) A^{-1} - (-1)^M \beta^N \neq 0$$

for n sufficiently large. Thus the expression on the left hand side of inequality (8) is not equal to zero and we may apply Lemma 1 with $\alpha_1, \ldots, \alpha_n$ given by $-1, p_0, p_1, \ldots, p_k, \beta$ and A respectively. We may assume that $p_1, \ldots, p_k$ are all less than n^2 since otherwise the theorem is valid and therefore, from Lemma 1,

$$|(-1)^M p_0 p_1^{h_1} \ldots p_k^{h_k} \beta^{-N} A^{-1} - 1|_{\mathfrak{p}_j} > \exp\left(-c_2 (k \log n)^{c_3 k} \log V (\log B)^2\right), \tag{9}$$

where V denotes the height of A and B denotes the maximum of $2, M, h_1, \ldots, h_k$ and N. Some calculation shows, see [**5**: p. 442], that V is bounded above by $|\alpha|^{c_4 (\log n) d_s - 1}$ and that B is bounded above by $c_5 n^2$. Thus from (8), (9) and the product formula for valuations we obtain

$$|\text{Norm}\,(\alpha)|^{d_s} \leqslant \exp\left(c_6 (k \log n)^{c_7 k} d_{s-1}\right) \tag{10}$$

Note that $|\text{Norm}(\alpha)| > 1$ since α is non-zero and is not a unit. On comparing (6) and (10) we find that

$$k > c_8(\log n)/q(n)\log\log n\,,$$

and employing the Brun–Titchmarsh theorem for primes in the arithmetical progressions $\pm 1 \pmod n$ we obtain Theorem 1; details may be found in [5; pp. 442–443].

3. *Proof of Theorem* 2

The proof of Theorem 2 given in [5] for the case when α and β are real may be repeated for the case when α and β are complex. In fact the only changes required in the text of the proof of Theorem 2 in [5] for this purpose are the replacement of (19) and (21) by (6) and (29) by (10).

4. *Proof of Theorem* 3

We may assume without loss of generality that α and β are coprime and, since $\Phi_n(\alpha, \beta) = \Phi_n(\beta, \alpha)$ for $n > 2$, that $\alpha > |\beta| > 0$. Further, in view of Theorem 1, we may assume that α is at least $\exp(\exp(10))$, whence $\log\log\log\alpha$ is larger than one. Also we shall assume that n exceeds a sufficiently large number c_1, where $c_1, c_2, \ldots$ are positive numbers which are effectively computable in terms of $P(\alpha\beta)$ and κ only.

We have, see [1],

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

where $p_1, \ldots, p_k$ are distinct primes congruent to $1 \pmod n$ and p_0 is 1 or the greatest prime factor of n. We can assume that the primes $p_1, \ldots, p_k$ do not exceed n^2 and that k is at most $\log n$ since otherwise the theorem plainly holds. By (5) $\Phi_n(\alpha, \beta)$ divides $\alpha^n - \beta^n$ and thus

$$p_j^{-h_j} = |\Phi_n(\alpha, \beta)|_{p_j} \geqslant |\alpha^n - \beta^n|_{p_j} > 0\,,$$

for $j = 1, \ldots, k$. Write

$$\alpha = q_1^{a_1} \ldots q_s^{a_s} \quad \text{and} \quad \beta = q_0 q_1^{b_1} \ldots q_s^{b_s}\,,$$

where $a_1, \ldots, a_s, b_1, \ldots, b_s$ are non-negative integers, $q_0 = \pm 1$ and $q_1, \ldots, q_s$ are prime numbers. Put

$$Q = P(\alpha\beta) = \max\{q_1, \ldots, q_s\}\,.$$

Note that

$$\max\{a_1, \ldots, a_s, b_1, \ldots, b_s\} \leqslant 2\log\alpha\,, \tag{11}$$

and that $s < Q$. Since α and β are coprime the primes $q_1, \ldots, q_s$ are distinct from $p_1, \ldots, p_k$. Thus we have

$$0 < |q_0^{-n} q_1^{(a_1-b_1)n} \ldots q_s^{(a_s-b_s)n} - 1|_{p_j} \leqslant p_j^{-h_j}, \quad 1 \leqslant j \leqslant k.$$

We now employ Lemma 1 with $\alpha_1, \ldots, \alpha_n$ given by $q_0, q_1, \ldots, q_s$ respectively and p given by p_j. Note that $D = 1$, $n = s+1 \leqslant Q$ and $\Omega \leqslant c_2$. Furthermore $p = p_j \leqslant n^2$ and, by (11), $B \leqslant 2n \log \alpha$, whence

$$p_j^{h_j} \leqslant \exp\left(c_3 n^2 (\log n + \log\log \alpha)^2\right) \leqslant \exp\left(c_3 n^3 (\log\log \alpha)^2\right),$$

for $j = 1, \ldots, k$. Thus

$$\max\{h_1, \ldots, h_k\} \leqslant c_3 n^3 (\log\log \alpha)^2, \tag{12}$$

and

$$|\Phi_n(\alpha, \beta)| \leqslant n \exp\left(k c_3 n^3 (\log\log \alpha)^2\right),$$

which, since $k \leqslant \log n$, is

$$\leqslant \exp\left(c_4 n^4 (\log\log \alpha)^2\right). \tag{13}$$

Let $d_0 = 1$ and let $d_1 < d_2 < \ldots < d_t$ be all the positive divisors of n with $\mu(n/d_r) \neq 0$. Then there exists a positive integer s, depending on n, such that

$$d_s/d_{s-1} \geqslant \exp\{(\log n)/q(n)\} \tag{14}$$

$$\geqslant \exp\{(\log n)^{\lambda}\}, \tag{15}$$

where $\lambda = 1 - \kappa \log 2$. Define A, M and N as in the proof of Theorem 1 and proceed as before to obtain

$$0 < |(-1)^M p_0 p_1^{h_1} \ldots p_k^{h_k} q_0^{-N} q_1^{-b_1 N} \ldots q_s^{-b_s N} A^{-1} - 1|_{q_i} \leqslant |\alpha|_{q_i}^{d_s},$$

for those i with $1 \leqslant i \leqslant s$ for which $a_i > 0$. We now apply Lemma 1 with p given by q_i, $\alpha_1, \ldots, \alpha_n$ given by $-1, p_0, p_1, \ldots, p_k, q_0, \ldots, q_s$ and A respectively and with $n = k+s+4 \leqslant k+Q+4$ and $D = 1$. On recalling (11) and (12) and noting that $|N| \leqslant n^2$ we see that we can take $B = c_5 n^3 (\log \alpha)^2$ in Lemma 1. Finally on remarking that $s \leqslant t \leqslant 2^{\omega(n)} \leqslant \log n$ since $\kappa < 1/\log 2$, we find after a short calculation, that the height of A does not exceed $(2\alpha)^{(\log n) d_{s-1}}$ whence $\Omega \leqslant c_6 (2 \log n)^{k+2} (\log \alpha) d_{s-1}$. Therefore, by Lemma 1,

$$|\alpha|_{q_i}^{-d_s} \leqslant \exp\left(c_7 (k \log n)^{c_8 k} \log \alpha (\log\log \alpha)^2 d_{s-1}\right),$$

for $i = 1, \ldots, s$. Since $k < \log n$,

$$\alpha^{d_s} \leqslant \exp\left((\log n)^{c_9 k} \log \alpha (\log\log \alpha)^2 d_{s-1}\right),$$

and thus

$$d_s/d_{s-1} \leqslant (\log n)^{c_9 k} (\log\log \alpha)^2.$$

By (14) we have

$$\exp((\log n)/q(n) - c_9 k \operatorname{loglog} n) \leqslant (\operatorname{loglog} \alpha)^2 .$$

If $c_9 k \operatorname{loglog} n \geqslant \frac{1}{2}(\log n/q(n))$ then the theorem follows from the Brun–Titchmarsh theorem for primes in arithmetical progressions; here we consider the primes congruent to 1 modulo n. Accordingly we can assume that $c_9 k \operatorname{loglog} n \leqslant (\log n)/2q(n)$ whence

$$\exp\left((\log n)/2g(n)\right) \leqslant (\operatorname{loglog} \alpha)^2 .$$

From (14) and (15) we obtain

$$n \leqslant \exp\left((4 \operatorname{logloglog} \alpha)^{1/\lambda}\right).$$

Observe that $1/\lambda > 1$. We now conclude from (13) that

$$\log |\Phi_n(\alpha, \beta)| \leqslant c_4 \exp\left(6(4 \operatorname{logloglog} \alpha)^{1/\lambda}\right). \tag{16}$$

By assumption $\alpha > |\beta|$ and so $\alpha - |\beta| \geqslant 1$ since α and β are integers. Thus $|\alpha - \zeta^j \beta| \geqslant 1$ for any integer j and any root of unity ζ. Further if ζ is a primitive n-th root of unity and n is greater than 6 then $|\alpha - \zeta^j \beta| \geqslant |\alpha|$ for some integer j with $(j, n) = 1$. Therefore, from (1), we deduce that

$$\log |\Phi_n(\alpha, \beta)| \geqslant \log \alpha , \tag{17}$$

and a comparison of (16) and (17) reveals that $\alpha \leqslant c_{10}$. The theorem now follows immediately from Theorem 1.

References

1. G. D. Birkhoff and H. S. Vandiver, "On the integral divisors of $a^n - b^n$", *Ann. of Math.* (2), 5 (1904), 173–180.
2. A. J. van der Poorten, "Linear forms in logarithms in the p-adic case", *Transcendence theory: advances and applications* (ed. A. Baker and D. Masser, Academic Press, London, 1977).
3. A. Schinzel, "Primitive divisors of the expression $A^n - B^n$ in algebraic number fields", *J. Reine Angew. Math.*, 268/269 (1974), 27–33.
4. C. L. Stewart, "The greatest prime factor of $a^n - b^n$", *Acta Arith.*, 26 (1975), 427–433.
5. C. L. Stewart, "On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers", Proc. London Math. Soc. (3) 35, (1977), 425–447.
6. C. L. Stewart, "Primitive divisors of Lucas and Lehmer numbers", *Transcendence theory: advances and applications* (ed. A. Baker and D. Masser, Academic Press, London, 1977).

Department of Mathematics,
Panjab University,
Chandigarh 160014,
India.

and

Tata Institute of Fundamental Research,
Homi Bhabha Road,
Bombay 400005, India.

Department of Pure Mathematics,
University of Waterloo,
Waterloo, Ontario, Canada,
N2L 3G1.