ON THE EXISTENCE OF AN INFINITUDE OF COMPOSITE PRIMITIVE DIVISORS OF SECOND-ORDER RECURRING SEQUENCES

DOV AND MOSHE JARDEN
Hebrew University, Jerusalem, Israel

1. INTRODUCTION

Let $\alpha \neq 0$, $\beta = 0$, $|\alpha| > |\beta|$, be any two complex numbers, such that $\alpha + \beta$ and $\alpha\beta$ are two relatively prime integers. Then the numbers

$$D_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \beta^{n-1}, \quad S_n = \alpha^n + \beta^n$$

are integers, since they are expressed as rational integral symmetric functions of the roots α, β of an algebraic equation

$$z^2 - (\alpha + \beta)z + \alpha\beta = 0$$

with integral coefficients with leading coefficient unity. One may readily verify that $\{D_n\}$ and $\{S_n\}$ are second-order recurring sequences satisfying the common recursion relation

$$X_n = (\alpha + \beta)X_{n-1} - \alpha\beta X_{n-2} .$$

(Since $D_0 = 0$, $D_1 = 1$; $S_0 = 2$, $S_1 = \alpha + \beta$, the recursion relation again shows that the numbers D_n, S_n are integers.) One may also easily verify that $D_{2n} = D_n S_n$.

A divisor > 1 of D_n, $n > 1$, is said to be primitive (or: characteristic) if it is relatively prime to any D_i with $1 < i < n$. The greatest primitive divisor of D_n is denoted by D'_n. A divisor > 1 of S_n, $n > 1$, is said to be primitive (or: characteristic) if it is relatively prime to any S_i with $0 < i < n$. The greatest primitive divisor of S_n is denoted by S'_n. From $D_{2n} = D_n S_n$ one may easily deduce that

$$(1) \qquad D'_{2n} = S'_n .$$

(Received Nov. 1966--revised 1967)

For any prime p dividing a certain D_i with $i > 1$, a (p) denotes the smallest positive subscript n, such that $p | D_n$. Thus p is a primitive divisor of $D_{a(p)}$.

By F_n we denote the product

$$F_n = \prod_{d|n} D_d^{\mu\left(\frac{n}{d}\right)}, \tag{2}$$

where μ is the Moebius function.

R. D. Carmichael showed in [1] that for any $n \neq 4, 6, 12$ there is

$$D'_n = F_n \tag{3}$$

except when $n = a(p)p^\lambda$, p being a prime factor of D_n, $\lambda \geq 1$, in which case

$$D'_n = \frac{1}{p} F_n . \tag{4}$$

He showed furthermore that if $n = a(p)p^\lambda$, $\lambda > 1$, then p is the greatest divisor of n, except when $p = 2$, and $a(p) = 3$.

Furthermore Carmichael showed, for α, β real, the following inequalities

$$\alpha^{\phi(n)-2^{\omega(n)-1}} < F_n < \alpha^{\phi(n)+2^{\omega(n)-1}}$$

where ϕ is Euler's totient function, and $\omega(n)$ is the number of distinct prime factors of n.

The main result achieved by Carmichael is the following

Theorem XXIII. If α and β are real and $n \neq 1, 2, 6$, then D_n contains at least one characteristic factor, except when $n = 12$, $\alpha + \beta = \pm 1$, $\alpha\beta = -1$.

In the present paper the above Carmichael's results are generalized for any two complex numbers $\alpha \neq 0$, $\beta \neq 0$, $|\alpha| > |\beta|$, such that $\alpha + \beta$ and $\alpha\beta$ are two relatively prime integers. (However, the exact value of n beginning with which any D_n contains at least one characteristic factor, is not calculated here.) Furthermore, starting from (2), we deduce an asymptotic formula (6) for F_n which is stronger than the inequalities given by Carmichael. Finally, the method of proof used here is slightly simpler than the one used by Carmichael. The main results proved here are the existence of an infinitude of composite D'_n for any α, β; of composite D'_{2n} for $\alpha\beta \neq \square$; and of composite D'_{2n+1} for $(\alpha - \beta)^2 \neq \pm\square$, or $(\alpha - \beta)^2 = \square$ and $\alpha\beta \neq -\square$.

2. ASYMPTOTIC FORMULA FOR D'_n

By (2)

$$\log F_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log D_d = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log \frac{\alpha^d - \beta^d}{\alpha - \beta} = \log \alpha \sum_{d|n} \mu\left(\frac{n}{d}\right) d$$

$$+ \sum_{d|n} \mu\left(\frac{n}{d}\right) \log \left\{1 - \left(\frac{\beta}{\alpha}\right)^d\right\} - \log(\alpha - \beta) \sum_{d|n} \mu\left(\frac{n}{d}\right).$$

Noting that

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) d = \phi(n),$$

and

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) = 0$$

for any $n > 1$, we get

$$\log F_n = \log \alpha \cdot \phi(n) + \sum_{d|n} \mu\left(\frac{n}{d}\right) \log \left\{1 - \left(\frac{\beta}{\alpha}\right)^d\right\}, \quad \text{for any } n > 1. \tag{5}$$

Let us evaluate

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \log \left\{ 1 - \left(\frac{\beta}{\alpha}\right)^d \right\} .$$

Note that for any $0 < q < 1$ there exists a positive constant A, such that, for any complex z, for which $|z| \le q$, there is

$$|\log (1 + z)| \le A|z| ,$$

where by $\log (1 + z)$ the principal value of log is understood. Indeed,

$$\frac{\log (1 + z)}{z} = 1 - \frac{z}{2} + \frac{z^2}{3} - \cdots$$

is an analytic function in the circle $|z - 1| < q < 1$, hence it is bounded there. Now, putting $q = \left|\frac{\beta}{\alpha}\right|$, we have, for any $d > 1$, $\left|\frac{\beta}{\alpha}\right|^d \le q$. Hence

$$\left| \sum_{d|n} \mu\left(\frac{n}{d}\right) \log \left\{ 1 - \left(\frac{\beta}{\alpha}\right)^d \right\} \right| \le \sum_{d|n} \left| \log \left\{ 1 - \left(\frac{\beta}{\alpha}\right)^d \right\} \right| < \sum_{d=1}^{\infty} \left| \log \left\{ 1 - \left(\frac{\beta}{\alpha}\right)^d \right\} \right|$$

$$< A \sum_{d=1}^{\infty} \left|\frac{\beta}{\alpha}\right|^d = A\left|\frac{\beta}{\alpha}\right| \frac{1}{1 - \left|\frac{\beta}{\alpha}\right|} = A \frac{|\beta|}{|\alpha| - |\beta|} = B ,$$

where B is a positive constant.

Hence, by (5) it follows that

$$\log F_n = \log \alpha \cdot \phi(n) + 0(1) . \tag{6}$$

Now, by (3), (4), wu have the following

<u>Theorem 1.</u> There is

$$\log D'_n = \log \alpha \cdot \phi(n) + 0(1) , \tag{7}$$

except when $n = a(p)p^\lambda$, $\lambda \geq 1$, p being a prime factor of D_n', in which case it is

$$\text{(8)} \qquad \log D_n' = \log \alpha \cdot \phi(n) - \log p + 0(1) .$$

Now, by assumption, $\alpha\beta$ is an integer, and $|\alpha| > |\beta|$, therefore

$$|\alpha|^2 > |\alpha| \cdot |\beta| = |\alpha\beta| \geq 1 ,$$

hence

$$|\alpha| > 1, \quad |\log \alpha| \geq \log |\alpha| > 0 .$$

By a theorem in [2], p. 114, there exists a positive constant C, such that

$$\phi(n) > \frac{C \cdot n}{\log \log n} \quad \text{for } n > 3 .$$

On the other hand $p|n$, hence $\log p \leq \log n$. Hence, by Theorem 1,

$$\text{(9)} \quad \log D_n' > |\log \alpha| \cdot \phi(n) - \log p - B > \log|\alpha| \frac{C \cdot n}{\log \log n} - \log n - B \xrightarrow[n \to \infty]{} \infty,$$

which means that:

Theorem 2. Beginning with a certain positive n, D_n has at least one primitive factor.

Remark. The error term $0(1)$ in (7) cannot be refined, since if n is a prime, then

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \log\left\{1 - \left(\frac{\beta}{\alpha}\right)^d\right\} = -\log\left\{1 - \frac{\beta}{\alpha}\right\} + \log\left\{1 - \left(\frac{\beta}{\alpha}\right)^n\right\} \xrightarrow[n \to \infty]{} -\log\left\{1 - \frac{\beta}{\alpha}\right\} \neq$$

Theorem 3.

$$\sum_{n=1}^{\infty} \frac{1}{D'_n}$$

converges.

Proof. From (9) it follows that there is a positive constant D such that, for all $n \geq 1$,

$$D'_n \geq \frac{|\alpha|^{\frac{C \cdot n}{\log \log n}}}{e^B \cdot n} \geq D \cdot n^2$$

Hence

$$\sum_{n=1}^{\infty} \frac{1}{D'_n} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty.$$

3. MAIN RESULTS

Lemma 1. Be N the sequence of natural numbers, S a subsequence of N, and A a reduced arithmetic progression. Then, an infinitude of D'_n is composite for

I) $n \in S$ or II) $n \in N - S$

according as

I) any or II) no

prime member of A is a factor of a certain D'_n, $n \in S$.

Proof. I) Suppose any prime member of A is a factor of a certain D'_n. $n \in S$, and that there is a positive integer n_0 such that any D'_n, where $n \in S$, $n > n_0$, is a prime. Let q be the greatest prime factor of D'_n, $n \leq n_0$.

Then, by Theorem 3, and noting that

$$\sum_{p \in A} \frac{1}{p} = \infty ,$$

where p denotes a prime number, we have

$$\infty > \sum_{n \in N} \frac{1}{D'_n} \geq \sum_{n \in S} \frac{1}{D'_n} \geq \sum_{\substack{p \in A \\ p > q}} \frac{1}{p} = \infty ,$$

whence $\infty > \infty$, which is absurd. Thus, I) is proved.

II) Suppose no prime member of A is a factor of a certain D'_n, $n \in S$. Then, noting that any prime $p \nmid 2(\alpha - \beta)^2\alpha\beta$ is a factor of a certain D'_n ([1], p. 45, Theorem XII), any prime member of A not a factor of $2(\alpha - \beta)^2\alpha\beta$ ia a factor of a certain D'_n, $n \in N - S$, and II) follows as above.

Theorem 4. There is an infinitude of composite D'_n.

Proof. The theorem is an immediate consequence of Lemma 1, noting that any prime $p \nmid 2(\alpha - \beta)^2\alpha\beta$ is a factor of a certain D'_n.

Lemma 2. If b is an integer, and $b \neq \square$, then there exists an odd prime p, such that $\left(\frac{b}{p}\right) = -1$, where $\left(\frac{b}{p}\right)$ is Legendre's symbol. In particular,

I) If $b = \pm m^2 p_1, \cdots, p_r$, where $r \geq 1$ and $p_1, \cdots, p_r$ are distinct primes, then there exists an integer $u = 1 \pmod 4$, where $(u, 4p_1, \cdots, p_r) = 1$, such that, for any prime $p = u \pmod{4p_1, \cdots, p_r}$, it is

$$\left(\frac{\pm b}{p}\right) = -1 .$$

II) If $b = -m^2$, then for any prime $p = -1 \pmod 4$ it is

$$\left(\frac{b}{p}\right) = -1 .$$

Proof. [2], p. 75.

Lemma 3. Let p be an odd prime. If $p \mid ax^2 + by^2$ for some integers a, b, x, y, and $p \nmid (x, y)$, then

$$\left(\frac{-ab}{p}\right) = 1 \quad .$$

Proof. Since $p \nmid (x,y)$, p cannot divide both x and y. Thus, without loss of generality, we may assume that $p \nmid y$. Then there exists an integer z, such that $yz \equiv 1 \pmod{p}$. Hence, from $ax^2 + by^2 \equiv 0 \pmod{p}$ it follows that

$$(axz)^2 \equiv -ab \pmod{p},$$

whence

$$\left(\frac{-ab}{p}\right) = 1 \quad .$$

Lemmas 2, 3 imply the following:

Lemma 4. I) If $b = \pm m^2 p_1, \cdots, p_r$, where $r \geq 1$ and $p_1, \cdots, p_r$ are distinct primes, then there exists an integer $u \equiv 1 \pmod{4}$, where $(u, 4p_1, \cdots, p_r) = 1$, such that, for any prime $p \equiv u \pmod{4p_1, \cdots, p_r}$, it is $p \nmid x^2 + by^2$ for any integers x, y, such that $p \nmid (x, y)$.

II) If $b = m^2$ and $p \nmid (x,y)$, then $p \nmid x^2 + by^2$ for any prime $p \equiv -1 \pmod{4}$.

Theorem 5. If $\alpha\beta \neq \square$, then there is an infinitude of composite D^{1}_{2n}.

Proof. One may readily verify that

$$D_{2n+1} = D_{n+1}^2 - \alpha\beta D_n^2 \quad .$$

On the other hand, $(D_{n+1}, D_n) = 1$ ([1], p. 38, Corollary). Hence, putting in Lemma 4:

$$b = -\alpha\beta, \qquad x = D_{n+1}, \qquad y = D_n \quad ,$$

and noting that, according to the assumption, $b = -\alpha\beta \neq -\square$, there exists a reduced arithmetic progression A, no prime member of which divides D_{2n+r}.

Hence, no prime member of A is a factor of D'_{2n+1}. The theorem follows by Lemma 1, II).

Theorem 6. If

$$\text{I)} \qquad (\alpha - \beta)^2 \neq \pm\square ,$$

or

$$\text{II)} \qquad (\alpha - \beta)^2 = \square \quad \text{and} \quad \alpha\beta \neq -\square ,$$

then there is an infinitude of composite D'_{2n+1}.

Proof. One may readily verify that

$$S_n^2 = (\alpha - \beta)^2 D_n^2 + 4(\alpha\beta)^n . \tag{9}$$

I) Suppose that $(\alpha - \beta)^2 \neq \pm\square$. Then $(\alpha - \beta)^2 = \pm m^2 p_1, \cdots, p_r$, where $r \geq 1$ and $p_1, \cdots, p_r$ are distinct primes. Then, by Lemma 2, I), there is an integer u, such that

$$u = 1 \pmod 4 , \tag{10}$$

$$(u, 4p_1, \cdots, p_r) = 1 , \tag{11}$$

$$p = u \ (\mathrm{mod}\ 4p_1, \cdots, p_r) \tag{12}$$

implies

$$\left(\frac{-(\alpha - \beta)^2}{p}\right) = -1$$

for any prime p.

Consider the pair of congruences

$$\begin{cases} x = u \ (\mathrm{mod}\ 4p_1, \cdots, p_r) \\ x = 1 \ (\mathrm{mod}\ 4\alpha\beta) \end{cases} \tag{13}$$

From the identity

$$(\alpha + \beta)^2 - 4\alpha\beta = (\alpha - \beta)^2 ,$$

and from the assumption

$$(\alpha + \beta,\ \alpha\beta) = 1 ,$$

it follows

$$1 = (\alpha\beta, p_1, \cdots, p_r) \le (\alpha\beta,\ \pm m^2 p_1, \cdots, p_r) = (\alpha\beta, (\alpha - \beta)^2) = 1 .$$

Hence

$$(4p_1, \cdots, p_r, 4\alpha\beta) = 4(p_1, \cdots, p_r, \alpha\beta) = 4 .$$

But, by (10), $4 | u - 1$, hence (13) has a solution u', i.e.,

$$u' = u \pmod{4p_1, \cdots, p_r},\ u' = 1 \pmod{4\alpha\beta} . \tag{14}$$

Let p be a prime satisfying $p = 1 \pmod{4\alpha\beta}$. If $\alpha\beta$ is odd, then, according to the properties of the Jacobi symbol

$$\left(\frac{\alpha\beta}{p}\right) = \left(\frac{p}{\alpha\beta}\right) = \left(\frac{1}{\alpha\beta}\right) = 1 .$$

If $\alpha\beta$ is even, then $p = 1 \pmod 8$, and $\alpha\beta = 2^k t$, where $k \ge 1$ and $2 \nmid t$. Then

$$\left(\frac{\alpha\beta}{p}\right) = \left(\frac{2}{p}\right)^k \left(\frac{t}{p}\right) = \left(\frac{p}{t}\right) = \left(\frac{1}{t}\right) = 1 .$$

in both cases

$$\left(\frac{\alpha\beta}{p}\right) = 1 .$$

Combining the last result with (11), (12) and (14), we conclude

$$(15) \qquad (u', 4p_1, \cdots, p_r) = 1 ,$$

(16) If $p = u' \pmod{4p_1, \cdots, p_r}$, then

$$\left(\frac{-(\alpha - \beta)^2}{p}\right) = \left(\frac{-\alpha\beta(\alpha - \beta)^2}{p}\right) = -1 ,$$

for any prime p.

We shall now show that if

$$(17) \qquad p = u' \pmod{4p_1, \cdots, p_r} ,$$

then $p \not| D'_{2n}$. Indeed, if $p | D'_{2n}$, then, by (1), $p | S'_n$, hence $p | S_n^2$. Hence, by (9),

$$p \,|\, (\alpha - \beta)^2 D_n^2 + 4(\alpha\beta)^n .$$

Putting in Lemma 3:

$$x = D_n, \qquad y = 2, \qquad a = (\alpha - \beta)^2, \qquad b = (\alpha\beta)^n,$$

we have

$$\left(\frac{-(\alpha\beta)^n(\alpha - \beta)^2}{p}\right) = 1 .$$

If n is even, then

$$1 = \left(\frac{-(\alpha\beta)^n(\alpha - \beta)^2}{p}\right) = \left(\frac{-(\alpha - \beta)^2}{p}\right) ,$$

If n is odd, then

$$1 = \left(\frac{-(\alpha\beta)^n(\alpha - \beta)^2}{p}\right) = \left(\frac{-\alpha\beta(\alpha - \beta)^2}{p}\right) .$$

Both cases contradict (16). The theorem now follows from (17), (15), and Lemma 1, II).

II) Suppose $(\alpha - \beta)^2 = m^2$, where m is an integer and $\alpha\beta \neq -\square$. Then (9) becomes

$$S_n^2 = (mD_n)^2 + 4(\alpha\beta)^n \quad (18)$$

This formula implies, by Lemma 3, if

$$p \mid D'_{2n} \quad (19)$$

(and hence $p \mid S_n^2$), then

$$\left(\frac{-(\alpha\beta)^n}{p}\right) = 1 ,$$

for any odd prime p. Consider now the three following cases.

Case 1: $\alpha\beta = n^2 \cdot 2^k$, where $k \geq 0$. Then, if $p \equiv -1 \pmod 8$, then

$$\left(\frac{-(\alpha\beta)^n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^k = -1 ,$$

and hence, by (19), $p \nmid D'_{2n}$.

Case 2: $\alpha\beta = n^2 \cdot 2^k \cdot q_1, \cdots, q_r$, where $k \geq 0$, $r \geq 1$, $q_1, \cdots, q_r$ are distinct odd primes, and $t = q_1, \cdots, q_r \equiv 1 \pmod 4$.

Consider the pair of congruences

$$\begin{cases} x \equiv -1 \pmod 8 \\ x \equiv 1 \pmod t \end{cases} \quad (20)$$

Since $(t, 8) = 1$, (20) has a solution u. This solution satisfies

$$(u, 8t) = 1 . \quad (21)$$

If $p - u \pmod{8t}$ is a prime, then

$$(22) \qquad \left(\frac{-(\alpha\beta)^n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^{kn}\left(\frac{t}{p}\right)^n = -\left(\frac{1}{t}\right) = -1 ,$$

and hence, by (19), $p \not| D'_{2n}$.

Case 3: Everything as in Case 2, except that $t = -1 \pmod 4$.

Choose a quadratic nonresidue c modulo q_1, i.e.,

$$\left(\frac{c}{q_1}\right) = -1 .$$

Consider the system of congruences

$$(23) \qquad \begin{cases} x = -1 \pmod 8 \\ x = c \pmod{q_1} \\ x = 1 \pmod{q_2} \\ \cdots\cdots\cdots \\ x = 1 \pmod{q_r} \end{cases}$$

If $r \geq 2$, or the system

$$(24) \qquad \begin{cases} x = -1 \pmod 8 \\ x = c \pmod{q_1} \end{cases}$$

if $r = 1$. Since $q_1, \cdots, q_r$ are distinct odd primes, (23) and (24) have a solution v. v satisfies:

$$(25) \qquad (v,\ 8t) = 1 ,$$

If $p = v \pmod{8t}$ is a prime, then

$$(26) \qquad \left(\frac{-(\alpha\beta)^n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)^{kn}\left(\frac{t}{p}\right)^n = (-1)(+1)\left[-\left(\frac{p}{t}\right)\right]^n .$$
$$= -\left(-\left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right)\cdots\left(\frac{p}{q_r}\right)\right)^n$$
$$= -\left(-\left(\frac{c}{q_1}\right)\left(\frac{1}{q_2}\right)\cdots\left(\frac{1}{q_r}\right)\right)^n = 1 .$$

[Cont. on p. 406.]