ON THE NUMERICAL FACTORS OF THE ARITHMETIC FORMS $\alpha^n \pm \beta^n$.*

By R. D. Carmichael.

Let $\alpha + \beta$ and $\alpha\beta$ be any two relatively prime integers (different from zero). Then α and β are roots of the quadratic equation

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

It is obvious that the numbers D_n and S_n,

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

are integers, since they are expressed as rational integral symmetric functions of the roots of an algebraic equation with integral coefficients with leading coefficient unity. The principal object of the present paper is an investigation of the numerical factors of the numbers D_n and S_n. The case when α and β are roots of unity is excluded from consideration. (See § 2.)

The most valuable treatment of the questions connected with these numbers is that of Lucas.† The special case in which α and β are integers has been considered by Siebeck,‡ Birkhoff and Vandiver,§ Dickson,|| and Carmichael.¶

In Lucas's paper many results of interest and importance are obtained. The methods employed, however, are often indirect and cumbersome. In the present paper a direct and powerful method of treatment** is employed throughout; and in connection with the new results which are obtained many of Lucas's theorems are generalized and several errors†† in the statement of his conclusions are pointed out.

In § 1 several fundamental algebraic formulæ are obtained and a partial factorization of D_n and S_n is effected. In § 2 these algebraic formulæ are employed to derive numerous elementary properties of the integers

* Presented to the American Mathematical Society, December, 1912.

† American Journal of Mathematics, 1 (1878): 184–240, 289–321.

‡ Crelle's Journal, 33 (1846): 71–77.

§ *Annals of Mathematics*, (2) 5 (1904): 173–180.

|| American Mathematical Monthly, 12 (1905): 86–89.

¶ American Mathematical Monthly, 16 (1909): 153–159.

** Compare the method employed by Dickson in the paper already cited.

†† Compare the review of Lucas's paper in the Jahrbuch über die Fortschritte der Mathematik, 10 (1878): 134–136.

D_n and S_n relative to divisibility, and these properties are stated in explicit theorems.

In § 3 the important question of the appearance of a given prime factor in the sequence $D_1, D_2, D_3, \cdots$ is investigated. The principal results are contained in Theorems XII and XIII. Attention is called to the new number-theoretic functions introduced in connection with Theorem XIII and its corollary.

In § 4 a detailed study is made of the numerical factors of a set of numbers which are the values of an algebraic form $F_k(\alpha, \beta)$ which may be defined as that irreducible algebraic factor of $\alpha^k - \beta^k$ which is not a factor of any $\alpha^\nu - \beta^\nu$ for which $\nu < k$ (but see the definition in § 1). This investigation is fundamental in the study of the numbers D_n and S_n, and the results which are here obtained have important applications in the theory of numbers. Attention is called especially to Theorems XIV, XVI and XVIII.

In § 5 the theory of "characteristic factors" of F_n, D_n and S_n is developed.

In § 6 very simple proofs are given of certain special cases of Dirichlet's celebrated theorem concerning the prime terms of an arithmetical progression of integers; in particular, it is shown that there is an infinitude of prime numbers of each of the forms $4n + 1$, $4n - 1$, $6n + 1$, $6n - 1$.

In § 7 are given a number of theorems which are useful in the identification of large prime numbers. Among the results obtained the following two alone will be mentioned here: A necessary and sufficient condition that a given odd number p is prime is that an integer a exists such that

$$F_{p-1}(a, 1) \equiv 0 \bmod p;$$

a necessary and sufficient condition that $2^{2^n} + 1$, $n > 1$, is prime is that

$$3^{2^{2^n-1}} + 1 \equiv 0 \bmod 2^{2^n} + 1.$$

1. Notation. Fundamental Algebraic Formulæ.

Let

$$Q_n(x) = 0$$

be the algebraic equation whose roots are the primitive nth roots of unity without repetition, the coefficient of the highest power of x in $Q_n(x)$ being unity. The polynomial $Q_n(x)$ has all its coefficients integers; and it is of degree $\varphi(n)$, where $\varphi(n)$ denotes the number of integers not greater than n and prime to n.

From the theory* of the primitive roots of unity we have two formulæ

* See Bachmann's Kreistheilung, especially the third lecture.

which are fundamental for our purposes. Thus,

$$x^n - 1 = \prod_d Q_d(x), \tag{1}$$

where d ranges over all the divisors of n. Also,

$$Q_n(x) = \frac{(x^n - 1) \cdot \Pi(x^{n/p_ip_j} - 1) \cdots}{\Pi(x^{n/p_i} - 1) \cdot \Pi(x^{n/p_ip_jp_k} - 1) \cdots}, \tag{2}$$

where the p's denote the different prime factors of n and where the products denoted by Π extend over the combinations 2, 4, 6, $\cdots$ at a time of p_1, p_2, p_3, $\cdots$ in the numerator and over the combinations 1, 3, 5, $\cdots$ at a time in the denominator.

Let $\alpha + \beta$ and $\alpha\beta$ be any two relatively prime integers (different from zero); then α and β are the roots of the equation

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

whose coefficients $\alpha + \beta$ and $\alpha\beta$ are any two relatively prime integers both of which are different from zero. We shall exclude the trivial case $\alpha = \beta = 1$. It is then clear that α and β cannot be equal.

Now $\alpha^n + \beta^n$ represents an integer for every value of n, since the function $\alpha^n + \beta^n$ is a symmetric polynomial in α and β and has integral coefficients. On the other hand the function $\alpha^n - \beta^n$ does not necessarily have an integral value. If, however, this number is divided by $\alpha - \beta$ the result is clearly an integer, since it may obviously be written as a rational integral symmetric function of α and β with integral coefficients. Accordingly, let us define the integers D_n and S_n, for every value of n, by the relations

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

Then, obviously,

$$S_n = \frac{D_{2n}}{D_n},$$

so that a study of the factorization of the form D_n, for varying values of n, includes incidentally that of the form S_n. We shall therefore be interested primarily in the form D_n.

We define $F_k(\alpha, \beta)$ by the relation

$$F_k(\alpha, \beta) = \beta^{\phi(k)} Q_k(\alpha/\beta). \tag{3}$$

We shall now show that $F_k(\alpha, \beta)$ is an integer for every value of k except $k = 1$. The theorem is obviously true for $k = 2$; for,

$$F_2(\alpha, \beta) = \alpha + \beta.$$

Then suppose that k is greater than 2. Let ω be a primitive kth root of unity. Then evidently,

$$(4) \qquad F_k(\alpha, \beta) = \beta^{\phi(k)} Q_k(\alpha/\beta) = \prod_{i=1}^{\phi(k)} (\alpha - \omega^{s_i}\beta),$$

where for $i = 1, 2, \cdots, \varphi(k)$, the s_i are the $\varphi(k)$ positive integers less than k and prime to k. Hence

$$F_k(\alpha, \beta) = \prod_{i=1}^{\phi(k)} (\alpha - \omega^{s_i}\beta)\omega^{k-s_i},$$

since

$$\omega^{k-s_j} \cdot \omega^{k-s_i} = 1$$

when

$$s_j + s_e = k$$

and the factors in the above equation obviously fall into pairs such that the sum of the s's in each pair is k. Hence we see readily that

$$F_k(\alpha, \beta) = \prod_{i=1}^{\phi(k)} (\alpha\omega^{k-s_i} - \beta) = \prod_{j=1}^{\phi(k)} (\beta - \omega^{s_j}\alpha),$$

where in the last member s_j is written for $k - s_i$. By comparing this equation with (4) we find that

$$F_k(\alpha, \beta) = F_k(\beta, \alpha);$$

that is, $F_k(\alpha, \beta)$ is symmetric with respect to α and β. But it is a polynomial in α and β with integral coefficients. Hence we conclude that

The number $F_k(\alpha, \beta)$ is an integer for every value of k except $k = 1$.

Now from (1) we have readily

$$(5) \qquad D_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \prod_d{}' F_d(\alpha, \beta),$$

where d ranges over all the divisors of n except unity. *This important formula gives a (partial) factorization of the integer D_n.* Likewise, if ν is any divisor of n,

$$(6) \qquad D_{n/\nu} = \prod_\delta{}' F_\delta(\alpha, \beta),$$

where δ ranges over all the divisors of n/ν except unity. If now we divide the first of these equations by the second, member for member, we have

$$(7) \quad \frac{D_n}{D_{n/\nu}} = \alpha^{n(\nu-1)/\nu} + \alpha^{n(\nu-2)/\nu}\beta^{n/\nu} + \cdots + \alpha^{n/\nu}\beta^{n(\nu-2)/\nu} + \beta^{n(\nu-1)/\nu} = \prod_k F_k(\alpha, \beta),$$

where k ranges over all the divisors of n which are not at the same time divisors of n/ν.

From (2) we obtain readily the equation

$$(8) \qquad F_n(\alpha, \beta) = \frac{(\alpha^n - \beta^n) \cdot \Pi(\alpha^{n/p_ip_j} - \beta^{n/p_ip_j}) \cdots}{\Pi(\alpha^{n/p_i} - \beta^{n/p_i}) \cdot \Pi(\alpha^{n/p_ip_jp_k} - \beta^{p_ip_jp_k}) \cdots},$$

where the factors denoted by Π extend over the combinations 2, 4, 6, $\cdots$ at a time of $p_1, p_2, \cdots$ in the numerator and over the combinations 1, 3, 5, $\cdots$ at a time in the denominator. The total number of factors in the numerator of this equation is the same as that in the denominator; for, obviously, the first of these numbers is the sum of the positive terms and the second is the sum of the negative terms in the expansion of $(1-1)^r$ by the binomial formula, r being the number of different prime factors of n. Hence, dividing each of these factors in both numerator and denominator by $\alpha - \beta$, we have

$$(9) \qquad F_n(\alpha, \beta) = \frac{D_n \cdot \Pi D_{n/p_ip_j} \cdots}{\Pi D_{n/p_i} \cdot \Pi D_{n/p_ip_jp_k} \cdots},$$

where the products denoted by Π have a meaning similar to that above.

Let p be any prime factor of n and write

$$n = \nu p^a$$

where the exponent a is so chosen that ν is an integer which is not divisible by p. Consider the factors in the second member of (9) into which p does not enter explicitly; from (9) itself it is clear that these factors alone have the value $F_\nu(\alpha^{p^a}, \beta^{p^a})$. In the same way we see that the factors into which p enters explicitly have the value $1/F_\nu(\alpha^{p^{a-1}}, \beta^{p^{a-1}})$. Hence

$$(10) \qquad F_n(\alpha, \beta) = F_\nu(\alpha^{p^a}, \beta^{p^a}) \div F_\nu(\alpha^{p^{a-1}}, \beta^{p^{a-1}}).$$

Since

$$F_1(\alpha, \beta) = \alpha - \beta,$$

equation (10) may be used as a recursion formula for determining $F_n(\alpha, \beta)$. For $n \leqq 36$, Sylvester's table* of cyclotomic functions may conveniently be employed for finding $F_n(\alpha, \beta)$.

In passing we note without demonstration that (10) may be proved directly and then be employed for the derivation of (9).†

If, now, in equation (7) we replace n by $2n$, give to ν the value 2 and remember that

$$\frac{D_{2n}}{D_n} = S_n,$$

we have

$$(11) \qquad S_n = \alpha^n + \beta^n = \prod_k F_k(\alpha, \beta),$$

* American Journal of Mathematics, 2 (1879): 367–368.

† Compare Dickson, l. c., p. 86.

where k runs over all those divisors of $2n$ which contain 2 to the same power as $2n$ itself. *This important formula gives a (partial) factorization of the integer* S_n.

Let ν be any *odd* divisor of n; then, writing n/ν for n in (11) we have

$$S_{n/\nu} = \prod_k F_k(\alpha, \beta), \tag{12}$$

where k runs over all those divisors of $2n/\nu$ which contain 2 to the same power as $2n/\nu$ itself. Dividing (11) by (12), member for member, we have

$$\frac{S_n}{S_{n/\nu}} = \prod_k F_k(\alpha, \beta), \qquad \nu \text{ odd}, \tag{13}$$

where k runs over all those divisors of $2n$ which contain 2 to the same power as $2n$ itself and which do not divide $2n/\nu$.

2. General Properties of the Integers D_n and S_n Relative to Divisibility.

In view of the fact that a rational integral symmetric function of α, β with integral coefficients is an integer we have readily the two equations

$$(\alpha + \beta)^n = \alpha^n + \beta^n + \alpha\beta I_1 = S_n + \alpha\beta I_1,$$

$$D_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \alpha^{n-1} + \beta^{n-1} + \alpha\beta I_2 = S_{n-1} + \alpha\beta I_2,$$

where I_1 and I_2 are integers. Since $\alpha\beta$ and $\alpha + \beta$ are relatively prime integers it follows from the first of these equations that S_n is prime to $\alpha\beta$ for every value of n. Then from the second of the equations we conclude that D_n is likewise prime to $\alpha\beta$ for every value of n. Hence we have the following theorem:

THEOREM I. *The integers D_n and S_n are both prime to $\alpha\beta$.*

This theorem enables us to dispose of an exceptional case; namely, when $D_m = 0$ for some value of m. In this case $\alpha^m = \beta^m$ and hence

$$S_m = 2\alpha^m.$$

But S_m is prime to $\alpha\beta$ and hence to $\alpha^m\beta^m$. These two results agree only when

$$\alpha^m = \beta^m = \pm 1,$$

so that in this case α and β are both roots of unity. It is easy to see that S_k can assume no other value than -2, -1, 0, 1, 2; for

$$|S_k| \leqq |\alpha^k| + |\beta^k| = 2.$$

Now

$$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = \text{integer};$$

and hence

$$|\alpha - \beta| \gtreqqless 1,$$

since $\alpha \neq \beta$. Therefore

$$|D_k| \leqq |\alpha^k - \beta^k| \leqq |\alpha^k| + |\beta^k| = 2,$$

so that D_k can take only the values $-2, -1, 0, 1, 2$. A corresponding discussion can be made when $S_m = 0$ for some value of m, and with like results. The cases $D_m = 0$ for some m and $S_m = 0$ for some m are therefore both trivial. They arise when and only when α and β are roots of unity. Hence in what follows *we shall exclude from consideration the case in which α and β are roots of unity.* Then *D_m and S_m are always different from zero.*

Now

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

and hence

$$S_n^2 - (\alpha - \beta)^2 D_n^2 = 4\alpha^n\beta^n.$$

It is clear that $(\alpha - \beta)^2$ is an integer. Then from the above equation it follows that any common divisor of S_n^2 and D_n^2 must be a divisor of $4\alpha^n\beta^n$; but by Theorem I such a divisor is prime to $\alpha\beta$. Hence it is a divisor of 4. Therefore, either D_n and S_n are relatively prime or they have the greatest common divisor 2. That both of these cases may arise is shown by the following examples:

(1) $\alpha = 2, \beta = 1$. D_n and S_n have not the common divisor 2 and hence are relatively prime;

(2) $\alpha = 3, \beta = 1$. D_n and S_n have the common factor 2 if n is even.

Hence we have the following theorem:*

THEOREM II. *The integers D_n and S_n either are relatively prime or have the greatest common divisor* 2.

We shall now determine the character of D_n and S_n relative to divisibility by 2. From Theorem I it follows that both of them are odd when $\alpha\beta$ is even. Hence we have to treat further only the case when $\alpha\beta$ is odd. This will separate further into two cases according as $\alpha + \beta$ is odd or even. We start from the recurrence formulæ

$$(14) \qquad \begin{aligned} D_{n+2} - (\alpha + \beta)D_{n+1} + \alpha\beta D_n &= 0, \\ S_{n+2} - (\alpha + \beta)S_{n+1} + \alpha\beta S_n &= 0, \end{aligned}$$

which are readily verified by substituting for D_k and S_k, $k = n, n + 1, n + 2$, their values in terms of α and β. Since for the present discussion $\alpha\beta$ is odd, we have from (14)

$$D_{n+2} \equiv D_n, \qquad S_{n+2} \equiv S_n \mod 2$$

or

$$D_{n+2} \equiv D_{n+1} + D_n, \qquad S_{n+2} \equiv S_{n+1} + S_n \mod 2$$

according as $\alpha + \beta$ is even or odd.

* Lucas (l. c., p. 200) states inaccurately that D_n and S_n are relatively prime.

Now $D_1 = 1$ and $D_2 = \alpha + \beta$. Hence from the above congruences which involve D_n we see readily that when $\alpha + \beta$ is even D_n is even or odd according as n is even or odd; and that when $\alpha + \beta$ is odd, D_n is even or odd according as n is or is not a multiple of 3.

We treat the number S_n in a similar manner. We have

$$S_1 = \alpha + \beta, \qquad S_2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta.$$

Hence, if $\alpha + \beta$ is odd both S_1 and S_2 are odd; and if $\alpha + \beta$ is even both S_1 and S_2 are even. Therefore from the above congruences involving S_n we conclude readily that if $\alpha + \beta$ is even S_n is even for all values of n; and that if $\alpha + \beta$ is odd S_n is even or odd according as n is or is not a multiple of 3.

Collecting these results we have the following theorem:

THEOREM III. *If $\alpha\beta$ is even both D_n and S_n are odd. If $\alpha\beta$ is odd and $\alpha + \beta$ is even, then S_n is even for all values of n while D_n is even or odd according as n is even or odd. If both $\alpha\beta$ and $\alpha + \beta$ are odd then D_n and S_n are both even or both odd according as n is or is not a multiple of* 3.

From the properties of symmetric functions of the roots of an algebraic equation and the algebraic divisibility of D_n by D_ν when ν is a divisor of n, it follows immediately that the integer D_n is divisible by the integer D_ν when ν is a divisor of n. This is also an immediate consequence of equation (7); and the latter equation in general states more than this, that is, it gives a partial factorization of the integer D_n/D_ν. Thus we have the following theorem:

THEOREM IV. *If ν is a divisor of n then D_ν is a divisor of D_n and we have*

$$\frac{D_n}{D_\nu} = \prod_k F_k(\alpha, \beta),$$

where k ranges over all those divisors of n which are not at the same time divisors of ν.

For $\nu = 1$ this theorem gives a partial factorization of D_n, since $D_1 = 1$. In the preceding section we proved that the quantities $F_k(\alpha, \beta)$ have integer values.

By the aid of equation (13) the following theorem may be demonstrated:

THEOREM V. *If ν is a divisor of n such that n/ν is odd then S_n is divisible by S_ν and we have*

$$\frac{S_n}{S_\nu} = \prod_k F_k(\alpha, \beta),$$

where k runs over all those divisors of $2n$ which contain 2 to the same power as $2n$ itself and which do not divide 2ν.

From the identity

$$(\alpha^m - \beta^m)(\alpha^n + \beta^n) - (\alpha^n - \beta^n)(\alpha^m + \beta^m) = 2\alpha^n\beta^n(\alpha^{m-n} - \beta^{m-n}), \qquad m > n,$$

we have readily

$$D_m S_n - D_n S_m = 2\alpha^n\beta^n D_{m-n}. \tag{15}$$

From this equation and the fact that D_m and D_n are prime to $\alpha\beta$ it follows that every common *odd* divisor of D_m and D_n is also a divisor of D_{m-n}; whence we conclude readily that every common odd divisor of D_m and D_n is a divisor of D_ν where ν is the greatest common divisor of m and n. But according to Theorem IV D_ν is a divisor of D_m and D_n. Hence the greatest common divisor of D_m and D_n is D_ν provided that either D_m/D_ν or D_n/D_ν is odd. This latter fact we shall now prove by aid of Theorems I and III.

We have

$$\frac{D_m}{D_\nu} = \frac{\alpha^m - \beta^m}{\alpha^\nu - \beta^\nu} = \frac{\bar{\alpha}^{m/\nu} - \bar{\beta}^{m/\nu}}{\bar{\alpha} - \bar{\beta}},$$

if we replace α^ν, β^ν by $\bar{\alpha}$, $\bar{\beta}$. The last member of the above equation we denote by $\bar{D}_{m/\nu}$. We define $\bar{D}_{n/\nu}$ in a similar manner. It follows from Theorem I that $\alpha^\nu\beta^\nu$ and $\alpha^\nu + \beta^\nu$ are relatively prime. They are both different from zero. That is, $\bar{\alpha}\bar{\beta}$ and $\bar{\alpha} + \bar{\beta}$ are relatively prime integers both of which are different from zero. Hence we may apply Theorem III to $\bar{D}_{m/\nu}$ and $\bar{D}_{n/\nu}$. If $\bar{\alpha}\bar{\beta}$ is even both of these numbers are odd. If $\bar{\alpha}\bar{\beta}$ is odd and $\bar{\alpha} + \bar{\beta}$ is even one of the numbers $\bar{D}_{m/\nu}$ and $\bar{D}_{n/\nu}$ is odd; for either m/ν or n/ν is odd, since ν is the greatest common divisor of m and n. Likewise, if $\bar{\alpha}\bar{\beta}$ and $\bar{\alpha} + \bar{\beta}$ are both odd then one of the numbers $\bar{D}_{m/\nu}$, and $\bar{D}_{n/\nu}$, is odd; for either m/ν or n/ν is not divisible by 3, since ν is the greatest common divisor of m and n. Hence $\bar{D}_{m/\nu}$ and $\bar{D}_{n/\nu}$ have not the common factor 2.

Remembering that $\bar{D}_{m/\nu} = D_m/D_\nu$ and $\bar{D}_{n/\nu} = D_n/D_\nu$ and making use of the results of the last two paragraphs we have the theorem:*

THEOREM VI. *The greatest common divisor of D_m and D_n is D_ν where ν is the greatest common divisor of m and n.*

Since $D_1 = 1$ we have at once the following corollary:

COROLLARY. *The integers D_m and D_n are relatively prime when m and n are relatively prime.*

The example

$$S_6(2,\ 1) = 2^6 + 1 = 5.13, \qquad S_4 = 2^4 + 1 = 17, \qquad S_2 = 2^2 + 1 = 5$$

shows at once that the greatest common divisor of S_m and S_n is not always

* The part of this theorem which applies to the odd divisors of D_m and D_n is due to Lucas (l. c., p. 206).

S_ν where ν is the greatest common divisor of m and n. If, however, m/ν and n/ν are both odd this simple law obtains, as we now show. In this case it follows from Theorem V that S_ν is a common divisor of S_m and S_n. Now

$$D_{2m} = S_m D_m$$

and

$$D_{2n} = S_n D_n,$$

whence we conclude by aid of Theorem VI that the greatest common divisor of S_m and S_n is a factor of $D_{2\nu}$. Now

$$D_{2\nu} = S_\nu D_\nu$$

and hence we have only to examine what factors D_ν has in common with S_m and S_n. Now D_ν is a factor of D_m, and D_m and S_m have the greatest common divisor 1 or 2. Hence D_ν has with S_m and S_n the greatest common divisor 1 or 2. Therefore S_m and S_n have the greatest common divisor S_ν or $2S_\nu$; and in the next two paragraphs we show that the latter case does not arise.

To prove that the greatest common divisor under consideration is not $2S_\nu$ it is sufficient to show that either S_m/S_ν or S_n/S_ν is odd. This follows at once from Theorem III if $\alpha\beta$ is even; for then S_m and S_n are odd. In general

$$\frac{S_m}{S_\nu} = \frac{\alpha^m + \beta^m}{\alpha^\nu + \beta^\nu} = \frac{\bar{\alpha}^{m/\nu} + \bar{\beta}^{n/\nu}}{\bar{\alpha} + \bar{\beta}},$$

if $\alpha^\nu = \alpha$ and $\beta^\nu = \bar{\beta}$. Denote the last numerator above by $\bar{S}_{m/\nu}$ and define $\bar{S}_{n/\nu}$ in a similar way. Then Theorem III is applicable to $\bar{S}_{m/\nu}$ and $\bar{S}_{n/\nu}$. Now either m/ν or n/ν is prime to 3, and hence one of the numbers $\bar{S}_{m/\nu}$ and $\bar{S}_{n/\nu}$ is odd if $\bar{\alpha}\bar{\beta}$ and $\bar{\alpha} + \bar{\beta}$ are both odd, that is, if $\alpha\beta$ and $\alpha + \beta$ are both odd. In this case, then, one at least of the numbers S_m/S_ν and S_n/S_ν is odd.

Let us next consider the case in which $\alpha\beta$ is odd and $\alpha + \beta$ is even; say that $\alpha + \beta$ is an odd multiple of 2^k. Then, since

$$S_1 = \alpha + \beta$$

and

$$S_2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta,$$

it is easy to see that S_1 and S_2 are odd multiples of 2^k and 2 respectively. By means of the second recursion formula (14) one sees that in general S_n is an odd multiple of 2^k or of 2 according as n is odd or even. Hence in this case S_m/S_ν and S_n/S_ν are both odd, since m and ν and likewise n and ν are both odd or both even.

Thus we have the following theorem:

THEOREM VII. *If ν is the greatest common divisor of m and n, and m/ν and n/ν are both odd, then the greatest common divisor of S_m and S_n is S_ν.*

We turn now to an interesting theorem of a different character, namely:

THEOREM VIII. *Let $m_1, m_2, \cdots, m_s$ and $n_1, n_2, \cdots, n_r$ be two sets of positive integers which have the property that any positive integer d, different from unity, which is a factor of (just) t integers of the second set is also a factor of at least t integers of the first set; then the number*

$$\frac{D_{m_1} \cdot D_{m_2} \cdot \cdots \cdot D_{m_s}}{D_{n_1} \cdot D_{n_2} \cdot \cdots \cdot D_{n_r}}$$

is an integer.

This theorem is an immediate consequence of the (partial) factorization of D_n given in equation (5).

COROLLARY I. *The product of any n consecutive terms of the sequence $D_1, D_2, D_3, \cdots$ is divisible by the product of the first n terms.**

COROLLARY II. *The number*

$$\frac{D_1 D_2 \cdots D_{n_1+n_2+\cdots+n_k}}{(D_1 D_2 \cdots D_{n_1})(D_1 D_2 \cdots D_{n_2}) \cdots (D_1 D_2 \cdots D_{n_k})}$$

is an integer.

This result is analogous to the theorem that the polynomial coefficient

$$\frac{(n_1 + n_2 + \cdots + n_k)!}{n_1!\, n_2! \cdots n_k!}$$

is an integer.

Let m and n be any two relatively prime positive integers and suppose that the positive integer d ($d \neq 1$) is a divisor of s integers of the set $1, 2, \cdots, m$ and of t integers of the set $1, 2, \cdots, n$. Then d is obviously a divisor of at least $s + t$ integers of the set $1, 2, \cdots, m + n - 1$. In view of this fact Theorem VIII yields the further corollary:

COROLLARY III. *If m and n are any two relatively prime positive integers, then the number*

$$\frac{D_1 D_2 \cdots D_{m+n-1}}{(D_1 D_2 \cdots D_m)(D_1 D_2 \cdots D_n)}$$

is an integer.

This theorem is analogous to that which asserts that

$$\frac{(m + n - 1)!}{m!\, n!}$$

is an integer, provided that m and n are relatively prime.

* The result contained in this corollary is due to Lucas, who gave, however, a very different proof of it (Lucas, l. c., p. 203).

Similarly one may prove an extended analogue of the theorem which states that

$$\frac{(km_1)!\,(km_2)!\,\cdots\,(km_k)!}{m_1!\,m_2!\,\cdots\,m_k!\,(m_1+m_2+\cdots+m_k)!}, \qquad k \overline{\gtrless} 2,$$

is an integer, namely:

COROLLARY IV. *The number*

$$\frac{(D_1D_2\cdots D_{km_1})(D_1D_2\cdots D_{km_2})\cdots(D_1D_2\cdots D_{km_k})}{(D_1D_2\cdots D_{m_1})^{k-1}\cdots(D_1D_2\cdots D_{m_k})^{k-1}(D_1D_2\cdots D_{m_1+m_2+\cdots+m_k})}$$

is an integer.

Just as equation (5) was used in the demonstration of Theorem VIII we may employ equation (11) to prove the following theorem:

THEOREM IX. *Let $m_1, m_2, \cdots, m_s$ and $n_1, n_2, \cdots, n_r$ be two sets of positive integers such that every positive integer d which is a factor of (just) t of the numbers $n_1, n_2, \cdots, n_r$ with odd quotient is also a factor of at least t of the numbers $m_1, m_2, \cdots, m_s$ with odd quotient. Then the number*

$$\frac{S_{m_1}\cdot S_{m_2}\cdot\;\cdots\;\cdot S_{m_s}}{S_{n_1}\cdot S_{n_2}\cdot\;\cdots\;\cdot S_{n_r}}$$

is an integer.

COROLLARY. *The product of any $2n-1$ consecutive terms of the sequence $S_1, S_3, S_5, \cdots$ is divisible by the product of the first n terms.*

If m is any integer and q is any odd prime, it is obvious that there exist integers

$$a_1, a_2, \cdots, a_s, \qquad s = \frac{q-1}{2},$$

dependent on q alone, such that

$$\alpha^{mq} - \beta^{mq} = (\alpha^m - \beta^m)^q + a_1\alpha^m\beta^m(\alpha^m - \beta^m)^{q-2} + a_2\alpha^{2m}\beta^{2m}(\alpha^m - \beta^m)^{q-4} + \cdots + a_s\alpha^{sm}\beta^{sm}(\alpha^m - \beta^m);$$

whence

$$(16)\quad D_{mq} = (\alpha - \beta)^{q-1}D_m{}^q + a_1(\alpha-\beta)^{q-3}\alpha^m\beta^m D_m{}^{q-2} + \cdots + a_s\alpha^{sm}\beta^{sm}D_m.$$

Let us evaluate a_s. Since it is independent of α, β and m, we may choose any convenient values for these numbers. Then put $m = 1$, $\beta = 1$, $\alpha = r + 1$, where r is a positive integer to be chosen at convenience. Then from (16) we have

$$\frac{(r+1)^q - 1}{r} \equiv a_s(r+1)^s \bmod r.$$

If we suppose r to be a prime number different from q we see that a_s is not divisible by r. If we put $r = q^2$ it follows that a_s is divisible by q but not by q^2. Hence $a_s = q$.

Suppose now that D_m is divisible by p^λ, $\lambda \neq 0$, and by no higher power of p, p being a prime number; then from (16), since $a_s = q$, we have

$$(17) \qquad D_{mq} \equiv q\alpha^{sm}\beta^{sm}D_m \bmod p^{3\lambda}.$$

From this congruence it follows that $p^{\lambda+1}$ is the highest power of p contained in D_{mp}, provided that p is odd, and that p^λ is the highest power of p contained in D_{mq} when q is an odd prime different from p. We enquire further: What is the highest power of p contained in D_{2m}? We have $D_{2m} = D_m S_m$. In Theorem III we have seen that D_m and S_m have no common odd factor (different from unity). Hence, if p is an odd prime the highest power of p contained in D_{2m} is p^λ. If p is even, so that D_m is divisible by 2, it follows from Theorem III that S_m is divisible by 2. Then it follows from Theorem II that D_m and S_m have the highest common factor 2. Hence in this case D_{2m} contains $2^{\lambda+1}$; and it contains no higher power of 2 unless $\lambda = 1$.

These results lead to the following theorem:

THEOREM X. *If for $\lambda > 0$, $p^\lambda \neq 2$, p^λ is the highest power of a prime p contained in D_m then the highest power of p contained in $D_{m\mu p^a}$ is $p^{a+\lambda}$, μ being any number prime to p. If $p^\lambda = 2$, then $D_{m\mu 2^a}$ contains the factor 2^{a+1} and $D_{m\mu}$ is an odd multiple of 2.**

Suppose that S_m is divisible by p^λ, $\lambda > 0$, but by no higher power of the odd prime p. Then D_{2m} contains p^λ and no higher power of p, since

$$D_{2m} = D_m S_m$$

and D_m and S_m have no common odd prime factor. Therefore, according to the preceding theorem, $D_{2m\mu p^a}$, or $D_{m\mu p^a} \cdot S_{m\mu p^a}$, μ being prime to p, contains $p^{a+\lambda}$ and no higher power of p. Moreover $D_{m\mu p^a}$ and $S_{m\mu p^a}$ do not have a factor p in common. Hence one of these numbers contains $p^{a+\lambda}$ and no higher power of p while the other is prime to p. Since D_{2m} is a divisor of $D_{m\mu p^a}$ if μ is even, we see that $D_{m\mu p^a}$ contains $p^{a+\lambda}$ when μ is even. When μ is odd S_m is a factor of $S_{m\mu p^a}$ and hence in this case $S_{m\mu p^a}$ contains the factor $p^{a+\lambda}$.

Thus we have the following theorem:

THEOREM XI. *If p^λ, $\lambda > 0$, is the highest power of an odd prime p contained in S_m and μ is a number prime to p; then if μ is even $D_{m\mu p^a}$ is divisible by $p^{a+\lambda}$ and by no higher power of p and $S_{m\mu p^a}$ is prime to p, while if μ is odd $D_{m\mu p^a}$ is prime to p and $S_{m\mu p^a}$ is divisible by $p^{a+\lambda}$ and by no higher power of p.*

---

* The special case of this theorem in which $\mu = 1$ is given by Lucas (l. c., p. 210), but Lucas failed to notice the exceptional character of the case when $p^\lambda = 2$.

3. On the Appearance of a Given Prime Factor in the Sequence $D_1, D_2, D_3, \cdots$.

If it is known that a prime number p is a factor of D_m, theorems in the preceding section enable us to say how p enters into $D_{m\mu p^a}$. In the present section we show that any given prime p, which is not a factor of $\alpha\beta$, is a factor of a certain definite number of the sequence $D_1, D_2, D_3, \cdots$; we also carry out other related investigations. We have need of two lemmas, as follows:

LEMMA I. *If $S(\alpha^p, \beta^p)$ is any rational integral symmetric function of α^p, β^p with integral coefficients, then*

$$S(\alpha^p, \beta^p) \equiv S(\alpha, \beta) \bmod p,$$

p being a prime number.

The proof is not difficult. From Fermat's theorem it follows that

$$\alpha^p\beta^p \equiv \alpha\beta \bmod p, \tag{18}$$

since $\alpha\beta$ is an integer. Likewise

$$(\alpha + \beta)^p \equiv \alpha + \beta \bmod p.$$

But by the aid of the binomial formula we see that

$$(\alpha + \beta)^p \equiv \alpha^p + \beta^p \bmod p,$$

since the binomial coefficients for the prime exponent p are all multiples of p and $(\alpha + \beta)^p - (\alpha^p + \beta^p)$ is therefore clearly p times a polynomial which is symmetric in α, β and has integral coefficients; that is, $(\alpha + \beta)^p - (\alpha^p + \beta^p)$ is p times an integer. Hence

$$\alpha^p + \beta^p \equiv \alpha + \beta \bmod p. \tag{19}$$

But, since α^p and β^p are roots of the equation

$$x^2 - (\alpha^p + \beta^p)x + \alpha^p\beta^p = 0,$$

it is a consequence of the theory of symmetric functions of the roots of an algebraic equation that $S(\alpha^p, \beta^p)$ can be expressed in the form

$$S(\alpha^p, \beta^p) = P(\alpha^p + \beta^p, \alpha^p\beta^p),$$

where P is a polynomial in $\alpha^p + \beta^p, \alpha^p\beta^p$ with integral coefficients. From (18) and (19) it follows that

$$P(\alpha^p + \beta^p, \alpha^p\beta^p) \equiv P(\alpha + \beta, \alpha\beta) \bmod p.$$

But

$$P(\alpha + \beta, \alpha\beta) = S(\alpha, \beta)$$

and therefore

$$S(\alpha^p, \beta^p) \equiv S(\alpha, \beta) \bmod p,$$

as was to be proved.

If m is any integer and q is an odd prime, we have an identity of the form

$$(\alpha^m - \beta^m)^q = (\alpha^{qm} - \beta^{qm}) - q\alpha^m\beta^m(\alpha^{m(q-2)} - \beta^{m(q-2)}) + \cdots;$$

whence it follows that

$$(\alpha - \beta)^{q-1}D_m{}^q = D_{mq} + qI,$$

where I is an integer. Hence

$$D_{mq} \equiv (\alpha - \beta)^{q-1}D_m \bmod q.$$

Hence,

Lemma II. *If m is any integer and q is any odd prime, we have*

$$D_{mq} \equiv (\alpha - \beta)^{q-1}D_m \bmod q.$$

In particular,

$$D_{q^a} \equiv (\alpha - \beta)^{q-1}D_{q^{a-1}} \equiv \cdots \equiv (\alpha - \beta)^{a(q-1)}D_1 \bmod q.$$

Hence, since $D_1 = 1$, it follows that D_{q^a} is divisible by q when and only when $(\alpha - \beta)^2$ is divisible by q.

Theorem III gives exact information concerning the divisibility of D_n and S_n by 2. We shall now consider the question of the entrance of an odd prime factor q. If q is a factor of $\alpha\beta$ it follows from Theorem I that it does not divide either D_n or S_n. If it is a factor of $(\alpha - \beta)^2$ then it divides D_q, as we readily see from Lemma II. In what follows we shall consider the divisibility of D_n and S_n by an odd prime p which is not a divisor of either $(\alpha - \beta)^2$ or $\alpha\beta$.

If in equation (15) we put $m = p$ and $n = 1$ we have

$$D_pS_1 - D_1S_p = 2\alpha\beta D_{p-1},$$

or

$$(\alpha + \beta)D_p - S_p = 2\alpha\beta D_{p-1}.$$

From Lemma II it follows that

$$D_p \equiv (\alpha - \beta)^{p-1} \bmod p,$$

and from Lemma I that

$$S_p \equiv \alpha + \beta \bmod p.$$

Hence from the last equation we have

$$(\alpha + \beta)(\alpha - \beta)^{p-1} - (\alpha + \beta) \equiv 2\alpha\beta D_{p-1} \bmod p.$$

Now $(\alpha - \beta)^2$ is an integer; and therefore it follows from Fermat's theorem that

$$(\alpha - \beta)^{p-1} \equiv \pm 1 \bmod p.$$

Hence from the above congruence we have the two cases

$$D_{p-1} \equiv 0 \bmod p \quad \text{if} \quad (\alpha - \beta)^{p-1} \equiv 1 \bmod p,$$

$$\alpha\beta D_{p-1} \equiv -(\alpha + \beta) \bmod p \quad \text{if} \quad (\alpha - \beta)^{p-1} \equiv -1 \bmod p.$$

Now it is easy to verify that

$$D_{p+1} - (\alpha + \beta)D_p + \alpha\beta D_{p-1} = 0;$$

and hence we see that

$$D_{p+1} \equiv 0 \bmod p \quad \text{if} \quad (\alpha - \beta)^{p-1} \equiv -1 \bmod p.$$

Therefore we have the following theorem:*

THEOREM XII. *An odd prime p which does not divide either $(\alpha - \beta)^2$ or $\alpha\beta$ is a factor of D_{p-1} or of D_{p+1} according as $(\alpha - \beta)^{p-1}$ is congruent to $+1$ or to -1 modulo p.*

Obviously, if $\alpha - \beta$ is an integer (that is, if α and β are integers) we have always that D_{p-1} is divisible by p.

By means of Theorems X and XII we are now to prove a result of fundamental importance. In order to be able to state this result succinctly we shall employ a number-theory function $\lambda_{rs}(n)$ which we define below. It is convenient at the same time to define a second function $\varphi_{rs}(n)$ which is intimately related to $\lambda_{rs}(n)$.

Let rs and $r + s$ be any two integers; that is, let r and s be the roots of any quadratic equation of the form

$$x^2 - ux + v = 0$$

where u and v are integers. When p is an odd prime we define the symbol $\left(\frac{r,\, s}{p}\right)$ by the congruence

$$(r - s)^{p-1} \equiv \left(\frac{r,\, s}{p}\right) \bmod p,$$

it being understood that $\left(\frac{r,\, s}{p}\right)$ is the residue of least absolute value; whence $\left(\frac{r,\, s}{p}\right) = 0, +1,$ or -1 according as $(r - s)^2$ is divisible by p, is a quadratic residue of p, or is a quadratic non-residue of p. The symbol $\left(\frac{r,\, s}{2}\right)$ is defined thus:

$$\left(\frac{r,\, s}{2}\right) = 1, \text{ if } rs \text{ is even;}$$

$$\left(\frac{r,\, s}{2}\right) = 0, \text{ if } rs \text{ is odd and } r + s \text{ is even;}$$

$$\left(\frac{r,\, s}{2}\right) = -1, \text{ if } rs \text{ and } r + s \text{ are both odd.}$$

* This theorem is due to Lucas (l. c., pp. 290, 296, 297). Lucas's proof, however, is different from that above.

Then if

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where $p_1, p_2, \cdots, p_k$ are the different prime factors of n, we define $\varphi_{rs}(n)$ by the equation

$$\varphi_{rs}(n) = \prod_{i=1}^{k} p_i^{a_i-1}\left[p_i - \left(\frac{r, s}{p_i}\right)\right].$$

This function is similar to one introduced by Lucas, l. c., p. 300. It is, however, somewhat more general. For $r = 2$ and $s = 1$ we have

$$\varphi_{21}(n) = \varphi(n),$$

where $\varphi(n)$ is Euler's φ-function of n. The function introduced by Lucas does not have this interesting property of including the φ-function as a special case.

The functional value $\lambda_{rs}(n)$ is defined to be the least common multiple of the numbers

$$p_i^{a_i-1}\left[p_i - \left(\frac{r, s}{p_i}\right)\right], \qquad i = 1, 2, \cdots, k.$$

It is obvious that $\lambda_{rs}(n)$ is a divisor of $\varphi_{rs}(n)$.

The functions $\varphi_{rs}(n)$ and $\lambda_{rs}(n)$ have several important properties; but this is not an appropriate place to develop them in full.

The fundamental theorem to be proved may now be stated as follows:

THEOREM XIII. *If the number n,*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where $p_1, p_2, \cdots, p_k$ are the different prime factors of n, is prime to $\alpha\beta$ and if

$$\lambda = \lambda_{\alpha\beta}(n),$$

we have

$$D_\lambda \equiv 0 \bmod n.$$

To prove this theorem it is sufficient to show that D_λ contains the factor $p_i^{a_i}$ where i is any number of the set $1, 2, \cdots, k$. This follows at once from previous results. For, λ is a multiple of t_i,

$$t_i = p_i^{a_i-1}\left[p_i - \left(\frac{\alpha, \beta}{p_i}\right)\right] = p_i^{a_i-1} k_i,$$

say. From Theorems XII and III and the remark following Lemma II we see that D_{k_i} is in every case divisible by p_i; and hence from X that D_λ is divisible by $p_i^{a_i}$.

COROLLARY.* *If $\varphi = \varphi_{\alpha\beta}(n)$, then $D_\phi \equiv 0 \bmod n$.*

* This corollary is essentially the same as a certain fundamental result due to Lucas, l. c., p. 300. It should be noted that Lucas's statement of this theorem is not entirely accurate.

In connection with these simple theorems concerning the divisors of the numbers in the sequence $D_1, D_2, \cdots$, it should be noticed that no laws of corresponding simplicity obtain in the case of the sequence $S_1, S_2, \cdots$. We have seen that an odd prime p which does not divide either $(\alpha - \beta)^2$ or $\alpha\beta$ is a factor of D_{p-1} or of D_{p+1}. But in the case of the sequence $S_1, S_2, \cdots$ it often happens that a given prime number is not a factor of any term. Thus 7 is not a factor of $S_n(2, 1), \equiv 2^n + 1$, for any value of n. More generally, suppose that D_k, where k is odd, has an odd prime factor p while p is not a divisor of any D_ν for ν less than k. From Theorem VI it follows that D_m is divisible by p when and only when m is a multiple of k. If we suppose that p is a divisor of S_n for any given value of n we shall be led to a contradiction. For, since $D_{2n} = D_n S_n$, D_{2n} is divisible by p; and therefore $2n$ is a multiple of k. But k is odd, and hence n is a multiple of k. Therefore D_n is divisible by p; and D_n and S_n have the common odd prime factor p, which is impossible. Hence, *an odd prime number p which divides D_k, where k is odd, and does not divide any D_ν for ν less than k, is not a factor of any S_n.*

4. On the Numerical Factors of the Forms $F_k(\alpha, \beta)$.

We have already seen that the numbers $F_k(\alpha, \beta)$ are of fundamental importance in the factorization of D_n and S_n. We turn therefore to a detailed treatment of these numbers.

Let us suppose that

$$F_\nu(\alpha, \beta) \equiv 0 \bmod p, \qquad \nu > 1,$$

and that ν is not a multiple of the prime number p. Suppose that k is a subscript for which

$$F_k(\alpha, \beta) \equiv 0 \bmod p.$$

Now* F_ν and F_k are divisors of D_ν and D_k respectively, while the greatest common divisor of D_ν and D_k is D_δ, where δ is the greatest common divisor of ν and k. If we suppose that δ is different from ν we shall be led to a contradiction; for, F_ν is then a factor of D_ν/D_δ, as we see from (5), whereas from Theorem X it follows that D_ν/D_δ is not divisible by p since p is a factor of D_δ and ν/δ is prime to p. Hence $\delta = \nu$; and therefore k is a multiple of ν.

We shall now show that $F_{\nu p^a}(\alpha, \beta)$, $a > 0$, is divisible by p but not by p^2, except that when $p = 2$, $\nu = 3$, F_6 may be divisible by 2^2. [From Theorem III it follows that F_6 is divisible by 2.] If we suppose that we do not have simultaneously $p = 2$, $\nu = 3$, $a = 1$, we may proceed as follows: From

* When no confusion can arise we sometimes write F_ν for $F_\nu(\alpha, \beta)$.

Theorem IV we have

$$\frac{D_{\nu p^a}}{D_{\nu p^{a-1}}} = \prod_i F_i(\alpha, \beta),$$

where i ranges over those divisors of νp^a which contain the factor p^a. From Theorem X it follows that the first member of this equation is divisible by p but not by p^2. Hence (only) one of the numbers $F_i(\alpha, \beta)$ of the second member is divisible by p and it is not divisible by p^2. Suppose that this number is that for which $i = k$. Then k is a multiple of p^a. But from the discussion in the preceding paragraph we see that k is a multiple of ν. Hence $k = \nu p^a$, since this is the only common multiple of ν and p^a occurring as a subscript in the second number of our equation.

From this we conclude that each of the numbers $F_{\nu p}, F_{\nu p^2}, \cdots$ contains the factor p but that no one of them contains p^2, except that when $p = 2$, $\nu = 3$, F_6 may contain 2^2.

Now consider the number $F_{\nu\mu p^a}$, where μ is greater than unity and is prime to p. It is a divisor of $D_{\nu\mu p^a}/D_{\nu p^a}$; and from X it follows that the latter number is not divisible by p. Hence $F_{\nu\mu p^a}$ is prime to p.

Let us suppose that F_1^2, $\equiv (\alpha - \beta)^2$, is divisible by the odd prime p. From the remark following Lemma II we see that each of the numbers $F_p, F_{p^2}, \cdots$ is divisible by p. Just as in the preceding argument we may show that no one of the numbers $F_{p^2}, F_{p^3}, \cdots$ is divisible by p^2, and that $F_{\mu p^a}$ is not divisible by p if μ is greater than 1 and is prime to p and $a > 0$. The example

$$\alpha = 1 + \sqrt{6}, \quad \beta = 1 - \sqrt{6}, \quad (\alpha - \beta)^2 = 24, \quad F_3 = \alpha^2 + \alpha\beta + \beta^2 = 9$$

shows that F_1^2 may be divisible by p while F_p is at the same time divisible by p^2. If μ is greater than 1 and is prime to p and if further F_μ is divisible by p, we see at once that D_μ and D_p are both divisible by p — contrary to the corollary to Theorem VI, which asserts that D_μ and D_p are relatively prime since μ and p are relatively prime. Hence F_μ is not divisible by p.

Now suppose that F_1^2 is divisible by 2. Then, since

$$F_1^2 = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta$$

it follows that $\alpha + \beta$ is divisible by 2. That is, F_2 is divisible by 2. The example $\alpha = 2^k + 1$, $\beta = 2^k - 1$ shows that F_2 may be divisible by any power of 2 whatever. By means of the relation

$$F_{2^a} = \alpha^{2^{a-1}} + \beta^{2^{a-1}} = (\alpha^{2^{a-2}} + \beta^{2^{a-2}})^2 - 2\alpha^{2^{a-2}}\beta^{2^{a-2}}$$

it may be proved, however, that F_{2^a}, $a > 1$, is divisible by 2 but not by 2^2.

To be continued.