The Number Theory of a System of Hyperbolic Complex Numbers.

By

George C. Cree.

Submitted in Partial Fulfilment of the requirements for the degree of Master of Arts.

Oct. 1949.

I am grateful to Professor Williams for his invaluable suggestions and expert criticism.

CONTENTS.

Part 1

Some Aspects of Hyperbolic Trigonometry

Introduction

1) Arithmetical Definition of Hyperbolic Complex Numbers.

2) Geometric Representations and Consequences. Analogue of DeMoivre's Theorem for Hyperbolic Complex Numbers.

3) Definition of the Hyperbolic Functions in Quadrant A.

Part 2

The Number Theory of Hyperbolic Complex Numbers.

Introduction.

1) Numbers of F(j); Conjugate and Norm of a Number.

2) Equation Satisfied by Rational Numbers of F(j).

3) Integers of F(j).

4) New Notation for Integers.

5) Basis of F(j).

6) Discriminant of F(j).

7) Divisibility of Integers; Units and Associated Integers of F(j).

8) Prime Numbers of F(j) and Simple Factorization.

9) Unique Factorization Theorem for F(j).

10) Factorization and Representation of Integers as the Difference of Square

11) Congruences in F(j).

12) The Φ Function in F(j).

13) The Analogue in F(j) of Fermat's Theorem.

14) Primitive Roots of Congruences.

15) Quadratic Residues and Remarks Concerning Quadratic Reciprocity.

Bibliography.

INTRODUCTION

Although much has been written and a great deal of elegent theory developed for numbers of the form $x + iy$, where $i^2 = -1$ and x and y are real numbers, viz, the ordinary complex numbers; very little has been said concerning an analogous system of numbers of the form $x + jy$ where $j^2 = 1$. This system we shall term the "Hyperbolic Complex Numbers", due to their connection with the hyperbola and the hyperbolic functions. The purpose of this paper will be to develop the number theory properties of this system.

However, before proceeding to the direct investigation of this theory, it is perhaps advisable to develop some of the geometric and trigonometric aspects of these numbers in the manner which is usually followed in the introduction to ordinary complex numbers. We first build up the algebra of these numbers by the use of number couples; then proceed to develop a representation of these numbers in terms of hyperbolic functions, prove a theorem analogous to that of De Moivre for ordinary complex numbers, and finally outline a trigonometry for these hyperbolic numbers. For convenience, in the subsequent discussion we shall employ Roman letters for real numbers (including rational numbers and rational integers), and Greek letters for hyperbolic numbers (and also for hyperbolic integers).

Part 1

Some Aspects of Hyperbolic Trigonometry

1. ARITHMETICAL DEFINITION OF HYPERBOLIC COMPLEX NUMBERS.

The following purely arithmetical theory of couples or bipartite numbers of the form (a_1 , a_2), where a_1 and a_2 are real numbers, lays a logical foundation for these hyperbolic numbers.

Definition of equality of number couples :- Two couples (a_1 , a_2) and (b_1 , b_2) are equal if and only if $a_1 = b_1$ and $a_2 = b_2$. We notice that $(a_1 , a_2) \neq (a_2 , a_1)$ unless $a_1 = a_2$.

Definition of the negative of a number couple :- If $\alpha = (a_1 , a_2)$, then, by definition $-\alpha = -(a_1 , a_2) = (- a_1 , - a_2)$.

Addition, subtraction and multiplication of two couples and of a scalar by a number couple are defined by the following formulae,

$$\alpha + \beta = (a_1 , a_2) + (b_1 , b_2) = (a_1 + b_2 , a_2 + b_2)$$

$$\alpha - \beta = (a_1 , a_2) - (b_1 , b_2) = (a_1 , a_2) + (- b_1 , - b_2)$$

$$\alpha . \beta = (a_1 , a_2) . (b_1 , b_2) = (a_1 b_1 + a_2 b_2 , a_1 b_2 + a_2 b_1)$$

$$K . \alpha = k (a_1 , a_2) = (ka_1 , ka_2)$$

Addition is seen to be commutative and associative :

$\alpha + \beta = \beta + \alpha$, and $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ where α , β , γ are any number couples. Moreover, it is easy to show that multiplication is commutative, associative and distributive with respect to addition :

$$\alpha . \beta = \beta . \alpha \quad , \quad (\alpha . \beta) . \gamma = \alpha . (\beta . \gamma)$$

$$\alpha . (\beta + \gamma) = \alpha\beta + \alpha\gamma$$

Furthermore, for the sum of a number and its negative we have,

$$(a_1 , a_2) + (- a_1 , - a_2) = (0 , 0) \text{ and further}$$

$$\alpha + (0 , 0) = (a_1 , a_2) + (0 , 0) = (a_1 , a_2) = \alpha ,$$

Hence, in view of these relations, we shall write $(0 , 0) = 0$ when there is no possibility of misunderstanding. Also,

$$\alpha \cdot (1 , 0) = (a_1 , a_2).(1 , 0) = (a_1 , a_2) ;$$

thus (1 , 0) has the property of unity and we write 1 for it.

Division is defined as the operation inverse to multiplication. Division, except by (0 , 0) and any multiple of (1 , 1), is always possible and unique as follows,

$$\frac{(b_1 ,b_2)}{(a_1 ,a_2)} = \frac{(b_1 ,b_2)\,(a_1 ,-a_2)}{(a_1 ,a_2)\,(a_1 ,-a_2)} = \left(\frac{b_1a_1 - b_2a_2}{a_1^2 - a_2^2} , \frac{b_2a_1 - a_2b_1}{a_1^2 - a_2^2} \right)$$

In particular, we have

$$(a_1 ,0) \pm (b_1 ,0) = (a_1 \pm b_1 ,0); \quad (a_1,0).(b_1,0) = (a_1b_1 ,0) ;$$

$$\frac{(b_1 ,0)}{(a_1 ,0)} = \left(\frac{b_1}{a_1} ,0 \right) \qquad \text{provided } a_1 \neq 0.$$

Hence, the couples (a ,0) combine under the above definition of addition, multiplication, etc. exactly as the real numbers combine under ordinary addition, multiplication, etc. Thus we see that there is an isomorphism between the set of all couples (a , 0) whose second element is zero and the set of all real numbers a. Thus there is no ambiguity in writing a in place of (a , 0) for all real numbers a. For brevity, we write j = (0 , 1) then

$$j^2 = (0 , 1) \cdot (0 , 1) = (1 , 0) = 1$$

$$(a_1 ,a_2) = (a_1 ,0) + (0 ,a_2) = a_1 + a_2 \cdot (0 ,1) = a_1 + a_2\, j$$

The resulting symbol $a_1 + a_2\, j$ is called a hyperbolic complex number. The above definitions now assume the form:

$$(a_1 + a_2j) \pm (b_1 + b_2j) = (a_1 \pm b_1) + (a_2 \pm b_2)j.$$

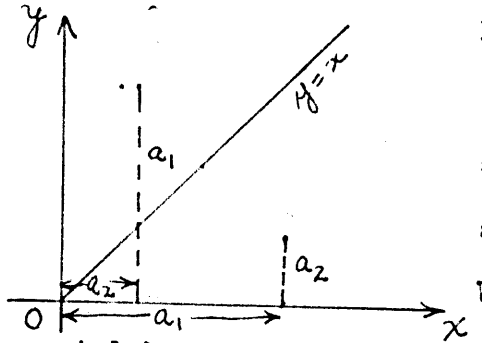
$$(a_1 + a_2j) \cdot (b_1 + b_2j) = (a_1b_1 + a_2b_2) + (a_1b_2 + a_2b_1)j$$

$$\frac{b_1 + b_2j}{a_1 + a_2j} = \frac{a_1b_1 - a_2b_2}{a_1^2 - a_2^2} + \frac{a_1b_2 - a_2b}{a_1^2 - a_2^2}\, j$$

where in the latter case, $(a_1 + a_2j) \neq 0$ and $a_1 \neq a_2$

2. GEOMETRIC REPRESENTATION AND CONSEQUENCES, De MOIVRE'S THEOREM.

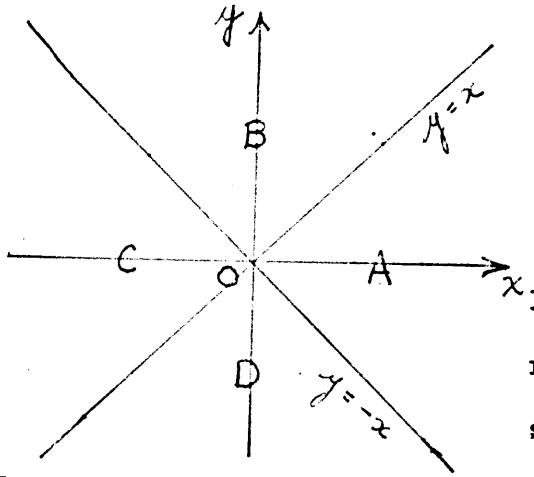
These numbers admit of a representation in a plane just as do ordinary complex numbers. Thus, if in the couple (a_1, a_2) we put $x = a_1$ and $y = a_2$ then (a_1, a_2) becomes a point in the plane.



From the adjoining figure we notice that (a_1, a_2) and (a_2, a_1) where $(a_1 \neq a_2)$ are obtained from one another by reflexion about the line $y = x$.

We know that ordinary complex numbers represented in terms of the arguments and moduli are unique up to the multiples of 2π. In seeking similar results for hyperbolic complex numbers we may write tenatively $\alpha = a + bj = r(\cosh u + j \sinh u)$ the conjugate of which is $\bar{\alpha} = a - bj = r(\cosh u - j \sinh u)$ and if we multiply these two numbers together we obtain

$$\alpha\bar{\alpha} = r^2 = a^2 - b^2$$ therefore so long as $|a| > |b|$, we shall have a real positive value for $r = \sqrt{a^2 - b^2}$



In view of this we divide the plane into 4 quadrants by the lines $y = x$ and $y = -x$ as in the adjoining figure. This shows that the point (a, b) in the case above lies in quadrant A, and we shall restrict ourselves to this quadrant in the subsequent trigonometric discussion, although the extension to the other quadrants is not difficult. Upon equating the real and j-parts we obtain $a = r \cosh u$, $b = r \sinh u$, therefore $\tanh u = b/a$. This gives

$$\frac{e^u - e^{-u}}{e^u + e^{-u}} = b/a = k \text{ whence } e^{2u} = \frac{1+k}{1-k} > 0$$ so that there exists a unique real angle u which satisfies this equation.

This shows that there is a unique representation of α as $r(\cosh u + j \sinh u)$ where r and u are real, and that, since the hyperbolic functions are periodic in $2\pi i$, if we wish to include imaginary angles, then

$$r[\cosh(u + 2p\pi i) + j \sinh(u + 2p\pi i)],$$

where p is any rational integer. The quantity r which appears, we may term the pseudo-distance from the origin to the point (a , b) since it plays a role analogous to the modulus in the case of ordinary complex numbers, which is the distance from a point in the complex plane to the origin. Clearly, r is independent of direction. Now we examine multiplication and division of hyperbolic numbers expressed in this representation and write

$$\alpha = r(\cosh u + j \sinh u) \quad \text{and} \quad \beta = s(\cosh v + j \sinh v)$$

α and β being any two hyperbolic numbers in quadrant A. Then

$$\alpha.\beta = rs(\cosh u \cosh v + \sinh u \sinh v) + j(\cosh u \sinh v + \sinh u \cosh v)$$
$$= rs[\cosh(u + v) + j \sinh(u + v)].$$

Similarly, for division we have

$$\frac{\alpha}{\beta} = \frac{r(\cosh u + j \sinh u)}{s(\cosh v + j \sinh v)} \cdot \frac{(\cosh v - j \sinh v)}{(\cosh v - j \sinh v)}$$
$$= r/s(\cosh u \cosh v - \sinh u \sinh v) + j(\sinh u \cosh v - \cosh u \sinh v)$$
$$= r/s(\cosh(u - v) + j \sinh(u - v),$$

These expressions for hyperbolic numbers in terms of hyperbolic functions are similar to those for ordinary complex numbers in terms of circular functions. Since we restrict ourselves to quadrant A, r and s will be positive and real in every case, and u and v are unique real angles.

Theorem A :- The representation of $\alpha = a + bj$ in terms of $r(\cosh u + j \sinh u)$ is unique up to multiples of $2\pi i$

Proof :- If possible, let there be two representations of the same number, $\alpha = a + bj = r(\cosh u + j \sinh u) = r(\cosh v + j \sinh v)$, so that $r[(\cosh u - \cosh v) + j(\sinh u - \sinh v)] = 0$. Since $r \neq 0$, then

$\cosh u = \cosh v$ and $\sinh u = \sinh v$ by equating the real and j-parts. Hence $u = v + 2n\pi i$ where n is any rational integer. Therefore the representation is unique, mod $2\pi i$, since the hyperbolic functions are periodic with period $2\pi i$.

Furthermore, in view of the rules of multiplication and division given above, we may state the following analogue to De Moivre's Theorem, viz-

Theorem B :- If $\alpha = a + bj = r(\cosh u + j \sinh u)$ and lies in quadrant A, then $\alpha^n = (a + bj)^n = r^n(\cosh nu + j \sinh nu)$.

Proof :- By the multiplication rule we have,

$$\alpha . \beta = rs(\cosh (u + v) + j \sinh (u + v))$$

so that, if $\alpha = \beta$ this becomes,

$$\alpha^2 = (a + bj)^2 = r^2(\cosh 2u + j \sinh 2u).$$

Continuing in this manner, we obtain for all positive integral values of n, the formula,-

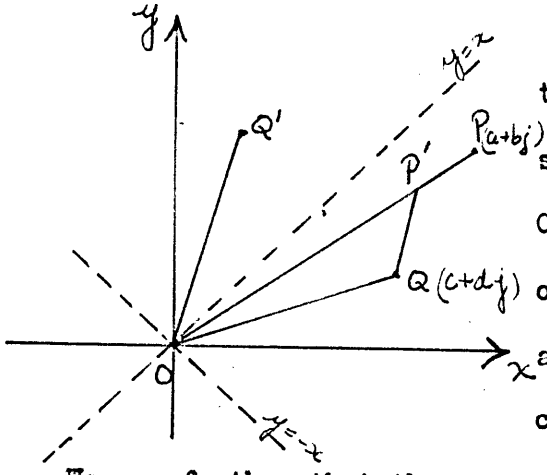
$$\alpha^n = \left[r(\cosh u + j \sinh u)\right]^n = r^n(\cosh nu + j \sinh nu)$$

which is the hyperbolic analogue of De Moivre's formula for ordinary complex numbers.

It is clear from these considerations that the hyperbolic numbers are associated with the hyperbolic functions in a similar manner to that in which the ordinary complex numbers are associated with the circular functions; hence the nomenclature adopted at the beginning of this paper.

3. DEFINITION OF THE HYPERBOLIC FUNCTIONS OF ANGLES IN QUADRANT A.

We now proceed to define the hyperbolic functions of angles in quadrant A, in a manner analogous to the definition of the circular functions in the first quadrant, i.e. in terms of the sides of a right triangle. Let us consider any two points P and Q in quadrant A. Then the vectors OP and OQ may be expressed as $a + bj$ and $c + dj$ respectively, where $a > |b| \geqslant 0$ and $c > |d| \geqslant 0$ as in the figure below.



Through Q draw QP' parallel to OQ', the reflection of OQ in the line $y = x$, so that QP' meets OP at P'. The vector OP' is easily seen to be the vector $k(OP)$ or $k(a + bj)$ where $k = \frac{c^2 - d^2}{ac - bd}$ which is always positive in virtue of the above conditions.

We see further that the pseudo-length (P.L.) of QP' is given by

$$\sqrt{\left[\left(\frac{c^2}{ac} \quad \frac{d^2}{bd}\right) \cdot a - c\right]^2 - \left[\left(\frac{c^2}{ac} \quad \frac{d^2}{bd}\right) \cdot b - d\right]^2} = i \left|\frac{bc - ad}{ac - bd}\right| \sqrt{c^2 - d^2}$$

the absolute value of $bc - ad$ being taken since this expression may be positive or negative. Furthermore, we define the directed pseudo-length (D.P.L.) of QP' as $i \frac{(bc - ad)\sqrt{c^2 - d^2}}{ac - bd}$. The quantity $bc - ad$ is just double the area of the triangle OQP, being positive if the vector OP, hence also OP', lies above OQ, and negative when OP lies below OQ. Let us consider the following ratios of the sides of the triangle OQP'-

$$C = \frac{(P.L.)\ OQ}{(P.L.)\ OP'} = \frac{ac - bd}{\sqrt{c^2 - d^2}\sqrt{a^2 - b^2}}$$

$$S = -i \frac{(D.P.L.)\ QP'}{(P.L.)\ OP'} = \frac{bc - ad}{\sqrt{c^2 - d^2}\sqrt{a^2 - b^2}}$$

Upon squaring and subtracting, we get $C^2 - S^2 = 1$; whence $C^2 = S^2 + 1$. Now, by definition, C is always positive and therefore must be $\geqslant 1$. S is positive or negative according as P' is above or below the vector OQ; i.e. according as u is measured a counterclockwise or clockwise direction. On this basis, we may write $C = \cosh u$ and $S = \sinh u$ and state the

Theorem C :- If OP and OQ are any two vectors in quadrant A, there is a triangle OQP' such that P and P' are collinear and QP' is the product of OQ by a scalar multiple of j. Furthermore, there is a uniquely determined real number u such that

$$\cosh u = \frac{(P.L.)\ OQ}{(P.L.)\ OP'}, \qquad \text{and} \qquad \sinh u = -i\frac{(D.P.L.)\ QP'}{(P.L.)\ OP'}$$

Thus we see that QP' plays the same role in hyperbolic trigonometry as the perpendicular in ordinary trigonometry, and, for this reason, we say that QP' is pseudo-perpendicular to OQ. This enables us to develop hyperbolic trigonometry in quadrant A in a manner analogous to the usual development of the trigonometry of the circular functions in the first quadrant.

However, as the purpose of this paper is to develop the number theory of this system of numbers, we shall conclude our discussion of hyperbolic trigonometry at this point and proceed to the main topics.

Part 2

The Number Theory of Hyperbolic Complex Numbers.

INTRODUCTION :- We now proceed to the investigation of the number theory problems connected with hyperbolic integers, and attempt, wherever possible, to establish results analogous to those for ordinary complex integers. As distinct from ordinary complex numbers, we note that the j-numbers do not form a field; but rather a ring since there are proper divisors of zero. In this system we have, as we saw previously, the two well defined operations of addition and multiplication; and, if we exclude zero and all the divisors of zero, we saw that a third operation,-division- was also possible. The ring consisting of all the hyperbolic complex numbers we denote by F(j). In the course of the subsequent discussion, we shall first establish several theorems concerning the whole ring F(j); define a convenient system of integers in F(j) and investigate their properties, and finally add a few remarks concerning a generalization of the quadratic reciprocity law to this system of integers.

1. NUMBERS OF F(j),- CONJUGATE AND NORM OF A NUMBER.

As we saw previously, any number of F(j) may be written in the form $a + bj$ where j satisfies the equation $x^2 - 1 = 0$, but no meaning is attached to j 'per se' , since this equation is clearly reducible in the real field, R. We say that the ring F(j) is characterized by this equation, and every number of F(j) is a rational function of j with real coefficients; and, since $j^2 = 1$, its degree in j may be reduced so as not to be higher than the first,

Definition :- The number $a - bj$ obtained by putting $-j$ for j in the number $\alpha = a + bj$ of F(j), is by definition the conjugate of α , and is denoted by $\bar{\alpha}$. Thus $3 + 2j$ and $3 - 2j$ are conjugate in F(j). Clearly a real number in this system, as in K(i), is its own conjugate.

Theorem 1 :- The conjugate of a product is equal to the product of the conjugates of the separate factors, i.e., if $\mu = \alpha\beta$ then $\bar{\mu} = \bar{\alpha}\bar{\beta}$.

Proof :- For if $\mu=\alpha\beta=(a+bj)(c+dj)=(ac+bd)+(bc+ad)j$, then we have $\bar{\mu}=(ac+bd)-(bc+ad)j=(a-bj)(c-dj)=\bar{\alpha}\,\bar{\beta}$; hence the desired result.

Definition :- We define the product of any number α of F(j) by its conjugate, as the norm of α and denote it by $n(\alpha)$. Thus

$$n(a+bj)=(a+bj)(a-bj)=a^2-b^2$$

Hence, the norm of a hyperbolic number $a+bj$ is zero if and only if the number itself is zero, or a divisor of zero; i.e. a multiple of $1+j$ or $1-j$. In fact $a^2-a^2=0$ is the norm of $a+aj=a(1+j)$ which is zero or a divisor of zero according as a is or is not equal to zero itself. Further, the norm of a number of F(j) may be any positive or negative real number or zero, as distinguished from the norms of ordinary complex numbers which are ≥ 0

Examples :- $n(3+2j)=(3+2j)(3-2j)=9-4=5$

$n(2+3j)=(2+3j)(2-3j)=4-9=-5$

$n(q(1+j))=0$, as we noted above.

Theorem 2 :- The norm of a product is equal to the product of the norms of its factors, i.e. $n(\alpha.\beta)=n(\alpha).n(\beta)$.

Proof :- For $n(\alpha.\beta)=\alpha\beta\,\bar{\alpha}\,\bar{\beta}=\alpha\bar{\alpha}\,\beta\bar{\beta}=n(\alpha).n(\beta)$.

Further, the cancellation law, viz, $\alpha\beta=\alpha\gamma$ implies that $\beta=\gamma$, is valid unless α is zero or a divisor of zero, for then it possesses an inverse $1/\alpha$ (division being defined if $\alpha\neq 0$ or a divisor of zero). Multiplying the equation $\alpha\beta=\alpha\gamma$ by this inverse, we get $\beta=\gamma$; however, no such inverse exists if α is a divisor of zero or zero itself, and the following example shows the result of using the law on divisors of zero. For

$$(1-j)2=(1-j)(1-j),\ \text{but}\ \ 2\neq 1-j$$

2. EQUATION SATISFIED BY THE RATIONAL NUMBERS OF F(j).

Definition :- A rational number of F(j) is one of the form $a+bj$ where a and b are rational numbers..

Every rational number α of F(j) satisfies a rational equation whose degree is the same as that of the ring itself, that is the second, and whose remaining root is the conjugate of α. The equation having as roots α and $\bar{\alpha}$ is $(x-(a+bj)).(x-(a-bj)) = x^2 - 2ax + a^2 - b^2$ and is therefore of the form $x^2 + px + q = 0$ with p and q rational numbers. If $b = 0$, so that $\alpha = \bar{\alpha}$, the equation is reducible in R being just $(x-a)^2 = 0$ and the equation of the lowest degree satisfied by α is $x - \alpha = 0$. If $b \neq 0$, that is $\alpha \neq \bar{\alpha}$, the second degree equation reducible, or not, over R satisfied by α is $x^2 - 2ax + a^2 - b^2 = 0$.

Hence the numbers of F(j) fall into two classes according as the equation satisfied by them is of the first or second degree. Those which satisfy equations of the same degree as that of the ring F(j), are called primitive numbers of the ring. Those which satisfy equations of lower degree than that of the ring are called imprimitive numbers of the ring. Clearly the imprimitive numbers of F(j), are just the rational numbers, and they are said to form a subfield of F(j). F(j) may be defined by one of its primitive numbers, but by none of its imprimitive ones. The middle and constant terms in the rational equation of lowest degree satisfied by α are seen to be trace α and norm α, where trace $\alpha = \alpha + \bar{\alpha}$ and norm $\alpha = \alpha.\bar{\alpha}$.

3. INTEGERS OF F(j).

To determine which numbers of F(j) are to take the place of integers, we must consider both the primitive and the imprimitive numbers of F(j), the latter being disposed of at once since a rational number is an algebraic integer if and only if it is a rational integer. To decide when a primitive number of F(j) is an integer, we shall, by definition, say that the necessary and sufficient condition that α be an integer of F(j), is that it satisfy an equation with integral coefficients of the form,

$x^2 + px + q = 0$ where $-p = \alpha + \bar{\alpha}$, $q = \alpha\bar{\alpha}$; that is, $\alpha + \bar{\alpha}$ and $\alpha.\bar{\alpha}$ must be rational integers.

If we write α (α not a divisor of zero) in the form $a + bj$ where $a = {}^{a_1}/_{c_1}$ and $b = {}^{b_1}/_{c_1}$; a_1, b_1, c_1 , being positive rational integers with no common factor, these conditions become,

(a) $\dfrac{a_1 + b_1 j}{c_1} + \dfrac{a_1 - b_1 j}{c_1} = \dfrac{2a_1}{c_1}$ = a rational integer.

(b) $\left(\dfrac{a_1 + b_1 j}{c_1}\right) \cdot \left(\dfrac{a_1 - b_1 j}{c_1}\right) = \dfrac{a_1^2 - b_1^2}{c_1^2}$ = a rational integer.

Thus, there are the following three possibilities,

(i) $c_1 > 2$ (ii) $c_1 = 2$ (iii) $c_1 = 1$

(i). If $c_1 > 2$, then, in virtue of (a), a_1 and c_1 would possess a common factor which, by (b), would be contained in b_1 also; a fact which is contrary to the hypothesis that a_1 is prime to c_1, and b_1 is prime to c_1. Thus, this case is impossible.

(ii). If $c_1 = 2$, then $a_1^2 - b_1^2$ must be divisible by 2^2, so that a_1 and b_1 must be either both even or both odd. The case of both even is clearly inadmissible since then a_1 and b_1 would possess a factor in common with c_1, contrary to the hypothesis that a_1 and b_1 were both prime to c_1. On the other hand, the case of a_1 and b_1 both being odd integers clearly satisfies both (a) and (b) above, and thus is possible.

(iii). If $c_1 = 1$ then both a_1 and b_1 are rational integers, and hence this case is also clearly possible.

We may summarize the above three cases in the following definition,-

Definition :- A number of the form $a + bj$ shall be an integer of $F(j)$ if and only if a and b are rational integers, or both halves of odd rational integers. This definition, although arbitrary in a sense, gives a number theory quite analogous to that for the rational integers.

If $b = 0$, we obtain the rational integers. Just as for the rational integers, it is easy to see that the sum and product of two integers of $F(j)$ are again integers, and hence they form a subring of $F(j)$.

4. NEW NOTATION FOR INTEGERS.:-

At this point we introduce a notation which will have far-reaching implications in, and will also simplify considerably, the proofs of many of the subsequent theorems. If we denote $\frac{1+j}{2}$ by ω and $\frac{1-j}{2}$ by $\bar{\omega}$, then we may establish the following,

Theorem 3 :- Any integer of F(j) may be expressed in one and only one way in the form $r\omega + s\bar{\omega}$ where r and s are rational integers.

Proof :- We first consider the case of $a + bj$ where a and b are rational integers. Then

$$a + bj = r\omega + s\bar{\omega} = r\left(\frac{1+j}{2}\right) + s\left(\frac{1-j}{2}\right)$$

Therefore $2a + 2bj = r + s + (r - s)j$ so that, by equating real and j-parts, we have $r + s = 2a$ and $r - s = 2b$; thus $2r = 2a + 2b$ and also $2s = 2a - 2b$, which give $r = a + b$ and $s = a - b$, so that both r and s are rational integers since a and b are.

Similarly, if a and b are both halves of odd integers, we have

$$\frac{p}{2} + \frac{q}{2}j = a + bj = r\omega + s\bar{\omega} = r\left(\frac{1+j}{2}\right) + s\left(\frac{1-j}{2}\right)$$

where p and q are odd rational integers. Thus $p + qj = r + s + (r - s)j$ and therefore as above we get, $r + s = p$ and $r - s = q$, hence it follows that $r = \frac{p+q}{2}$ and $s = \frac{p-q}{2}$. Now $p + q$ and $p - q$ are both even, since p and q are both odd, and hence divisible by 2; so that, as in the previous case, both r and s are integers. Thus any integer of F(j), say $a + bj$, may be expressed in the form $r\omega + s\bar{\omega}$ where r and s are rational integers. That this representation is unique is clear as follows- for let $r\omega + s\bar{\omega}$ and $u\omega + v\bar{\omega}$ be two representations of $a + bj$, so that $a + bj = r\omega + s\bar{\omega} = u\omega + v\bar{\omega}$; whence $(r - u)\omega = (v - s)\bar{\omega}$. But ω and $\bar{\omega}$ are mutually perpendicular unit vectors lying along $y = x$ and $y = -x$ respectively, so that the equation above is true only if $r - u = 0$ and $v - s = 0$. From these it follows that $r = u$, $v = s$, and thus the representation is unique.

The advantages of this notation are mainly in multiplication since the cross product terms are all zero, viz $\omega\,\bar{\omega} = 0$, since $\frac{(1+j)}{2}\cdot\frac{(1-j)}{2} = 0$ and $\omega + \bar{\omega} = 1$. Also it possesses the advantage that $\omega^n = \omega$, and $\bar{\omega}^n = \bar{\omega}$, so that to multiply two integers together we merely multiply the ω and $\bar{\omega}$ parts separately and add the results (i.e. $(a\omega + b\bar{\omega})(c\omega + d\bar{\omega}) = (ac\omega + bd\bar{\omega})$. Since ω and $\bar{\omega}$ are conjugates, the conjugate of an integer $a\omega + b\bar{\omega}$ is clearly formed by writing $\bar{\omega}$ for ω and ω for $\bar{\omega}$ giving conjugate $(a\omega + b\bar{\omega}) = a\bar{\omega} + b\omega$. The norm also assumes an especially simple form, as for example,

$$n(a\omega + b\bar{\omega}) = (a\omega + b\bar{\omega})(a\bar{\omega} + b\omega) = (ab)(\omega + \bar{\omega}) = ab$$

and so a number cannot have norm zero unless either of the coefficients of ω or $\bar{\omega}$ are zero or is simply zero itself (i.e. the divisors of zero are multiples of ω and $\bar{\omega}$.).

5. BASIS OF F(j).

Two integers α_1 and α_2 are said to form a basis of the integers F(j), if every integer can be represented in the form $a_1\alpha_1 + a_2\alpha_2$ where a_1 and a_2 are rational integers. (Clearly numbers of this form must be integers).

For example:- $3\omega + \bar{\omega}$, and $2\omega + \bar{\omega}$ form such a basis, for if

$$a\omega + b\bar{\omega} = a_1(2\omega + \bar{\omega}) + a_2(3\omega + \bar{\omega})$$

then $2a_1 + 3a_2 = a$; $a_1 + a_2 = b$ and solving these we find that a_1 and a_2 are rational integers as was required. We observe that the determinant of the coefficients of the basis is

$$\begin{vmatrix} 3 & 1 \\ 2 & 1 \end{vmatrix} = 1, \text{or } -1$$ if we reverse the order of the elements in the basis.

Theorem 4. If α_1 and α_2 be a basis of F(j), a necessary and sufficient condition that

$$(1) \qquad \begin{aligned} \alpha_1' &= a_1\alpha_1 + a_2\alpha_2 \\ \alpha_2' &= b_1\alpha_1 + b_2\alpha_2 \end{aligned} \qquad \text{where } a_1,\ a_2,\ b_1,\ b_2$$

are rational integers, shall be also a basis of $F(j)$ is

$$(2) \qquad \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \pm 1$$

Proof :- The necessity; for if α'_1, α'_2 be a basis we have

$$(3) \qquad \begin{aligned} \alpha_1 &= a'_1\alpha'_1 + a'_2\alpha'_2 \\ \alpha_2 &= b'_1\alpha'_1 + b'_2\alpha'_2 \end{aligned}$$

where a'_1, a'_2, b'_1, b'_2 are rational integers and substituting the values of α'_1, α'_2 from (1) into (3) we have

$$(4) \qquad \alpha_1 = (a'_1a_1 + a'_2b_1)\alpha_1 + (a'_1a_2 + a'_2b_2)\alpha_2$$

$$(5) \qquad \alpha_2 = (b'_1a_1 \quad b'_2b_1)\alpha_1 + (b'_1a_2 + b'_2b_2)\alpha_2$$

from which it follows that

$$a'_1a_1 + a'_2b_1 = 1 \; ; a'_1a_2 + a'_2b_2 = 0$$

$$b'_1a_1 + b'_2b_1 = 0 \; ; b'_1a_2 + b'_2b_2 = 1$$

whence

$$\begin{vmatrix} a'_1 & a'_2 \\ b'_1 & b'_2 \end{vmatrix} \cdot \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \begin{vmatrix} a'_1a_1+a'_2b_1 & b'_1a_1+b'_2b_1 \\ a'_1a_2+a'_2b_2 & b'_1a_2+b'_2b_2 \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

therefore

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \pm 1$$

The condition is also sufficient; for solving (1) for α_1 and α_2 we have, if (2) be satisfied, that,

$$\begin{aligned} \alpha_1 &= (b_1\alpha'_1 + a_2\alpha'_2) \\ \alpha_2 &= (b_1\alpha'_1 + a_1\alpha'_2) \end{aligned}$$

and hence if $\alpha = c_1\alpha_1 + c_2\alpha_2$ be any integer of $F(j)$ then

$$\alpha = (c_1b_2 + c_2b_1)\alpha'_1 + (c_1a_2 - c_2a_1)\alpha'_2$$

That is $\alpha = d_1\alpha'_1 + d_2\alpha'_2$ where d_1 and d_2 are integers. Since there is an infinite number of different sets of rational integers a_1, a_2, b_1, b_2, satisfying the relation

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \pm 1$$

there is an infinite number of bases of F(j).

As an example of this we may consider the change from the $a + bj$ notation to the $r\omega + s\bar{\omega}$ notation, as a change of basis. For then we have $a + bj = r(\omega + 0\bar{\omega}) + s(0\omega + \bar{\omega})$, and the determinant of the coefficients is

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1$$

as it should if ω and $\bar{\omega}$ are to be a basis of the integers of F(j).

6. DISCRIMINANT OF F(j).

The square of the determinant,

$$\begin{vmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha}_1 & \bar{\alpha}_2 \end{vmatrix}$$

formed from two basis numbers and their conjugates is called the discriminant of F(j), and is denoted by d. We easily verify that d is independent of the basis as follows,- for if α_1, α_2 and $\alpha'_1 = a_1\alpha_1 + a_2\alpha_2$, $\alpha'_2 = b_1\alpha_1 + b_2\alpha_2$ be any two bases, then

$$\begin{vmatrix} \alpha'_1 & \alpha'_2 \\ \bar{\alpha}'_1 & \bar{\alpha}'_2 \end{vmatrix}^2 = \begin{vmatrix} a_1\alpha_1 + a_2\alpha_2 & b_1\alpha_1 + b_2\alpha_2 \\ a_1\bar{\alpha}_1 + a_2\bar{\alpha}_2 & b_1\bar{\alpha}_1 + b_2\bar{\alpha}_2 \end{vmatrix}^2 = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}^2 \cdot \begin{vmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha}_1 & \bar{\alpha}_2 \end{vmatrix}^2 = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha}_1 & \bar{\alpha}_2 \end{vmatrix}^2$$

In fact, since $2\omega + \bar{\omega}$, and $3\omega + \bar{\omega}$ form a basis, then we have

$$\begin{vmatrix} 2\omega + \bar{\omega} & 3\omega + \bar{\omega} \\ 2\bar{\omega} + \omega & 3\bar{\omega} + \omega \end{vmatrix}^2 = 1$$

so that any two integers F(j) such that their discriminant is unity form a basis of F(j).

7. DIVISIBILITY OF INTEGERS; UNITS AND ASSOCIATED INTEGERS OF F(j).

Definition:- As in the case of rational integers, we say that α divides β or α is a factor of β (α and β both hyperbolic integers) if there exists another integer γ (α, β, γ not divisors of zero) such that $\alpha\gamma = \beta$; and we write $\alpha | \beta$. As usual, we do not define division by zero or by a divisor of zero. We now establish the,

Theorem 5 :- If α be divisible by β, then $n(\alpha)$ is divisible by $n(\beta)$.

Proof :- If $\alpha = \beta\gamma$, it follows from Theorem 1 that $n(\alpha) = n(\beta).n(\gamma)$,

and hence that $n(\alpha)$ is divisible by $n(\beta)$. However, the converse of this theorem is not, in general, true, as may be seen from the following simple example,- let $\alpha = 2\omega + \bar{\omega}$ and $\beta = \omega + 2\bar{\omega}$, then $n(\alpha) = 2$ and $n(\beta) = 2$ but α is not divisible by β.

Moreover, we cannot infer from the fact that $n(\alpha)$ divides $n(\beta)$ that α or $\bar{\alpha}$ is necessarily a factor of β. To show this, it will suffice to give a counter example, as follows,- let $n(\alpha) = 3.2 = 6$, and $n(\beta) = 6.5 = 30$.. Then $\alpha = 3\omega + 2\bar{\omega}$ and $\beta = 6\omega + 5\bar{\omega}$ and it may be shown by actual division that neither $3\omega + 2\bar{\omega}$ or $2\omega + 3\bar{\omega}$ is a factor of $6\omega + 5\bar{\omega}$.

In the rational field the integers ± 1, called units, are such that they divide every integer of the field. Obviously this property of ± 1 is carried over into F(j), however we must see whether there are any other integers in F(j) possessing this property. If there are any others, they must clearly be divisors of 1, and conversely, every divisor of 1 is a unit. Let $\varepsilon = a\omega + b\bar{\omega}$ be a unit of F(j); then $\alpha \cdot \varepsilon = \alpha$ where α is an integer of F(j). It follows that $n(\alpha)n(\varepsilon) = n(\alpha)$; hence $n(\varepsilon) = 1$ and further $n(\varepsilon) = ab = 1$. That $n(\varepsilon) = 1$ is not only necessary but also sufficient for ε to be a unit, is evident from the fact that from it follows $\varepsilon\bar{\varepsilon} = 1$ and hence $\bar{\varepsilon}$ is a divisor of 1. From the equation $ab = 1$ above, it follows that $a = \pm 1$ and $b = \pm 1$ whence the units are $\omega + \bar{\omega}$, $-\omega - \bar{\omega}$, $\omega - \bar{\omega}$, $-\omega + \bar{\omega}$, which are just 1, - 1, j, - j respectively. We observe that the above leads to three equivalent definitions of units:-

(i) They are divisors of 1.

(ii) They are integers whose reciprocals are integers.

(iii) They are integers whose norms are ± 1.

Definition :- Two integers α and β with no common divisors other than the units are said to be prime to each other.

Definition :- In the rational field, two integers m and $-m$ that

differ by a unit factor are said to be associated and similarily in F(j), the four integers $(a\omega + b\bar{\omega})$, $-(a\omega - b\bar{\omega})$, $(a\omega - b\bar{\omega})$, $-(a\omega + b\bar{\omega})$, obtained by multiplying the integer α by the four units are called associated integers. Any integer divisible by α is clearly also divisible by the associates of α.

8. PRIME NUMBERS OF F(j) AND SIMPLE FACTORIZATION.

By definition, an integer of F(j) that is not a unit and has no divisors other than its associates and the units, is called a prime number of F(j); all others being composite numbers. To determine whether an integer α, not a unit, is composite or prime; we need only examine its norm and we say that every number whose norm is a rational prime is a prime in F(j). For if we consider $\omega + p\bar{\omega}$ where p is a rational prime, and assume that it admits a decomposition into $a\omega + b\bar{\omega}$, and $c\omega + d\bar{\omega}$, then $\omega + p\bar{\omega} = (a\omega + b\bar{\omega})(c\omega + d\bar{\omega})$, so that

$n(\omega + p\bar{\omega}) = p = n\left[(a\omega + b\bar{\omega})(c\omega + d\bar{\omega})\right] = abcd$ and one of a,b,c, or d is equal to p and each of the others is either 1 or -1.

Similarly it may be shown that $p\omega + \bar{\omega}$ is also a prime of F(j), which is merely the conjugate of $\omega + p\bar{\omega}$. These results give the following

Theorem 6 :- A necessary and sufficient condition that an integer of F(j), should be a prime is that it possess a norm which is a rational prime.

That this condition is necessary has been shown above.
That it is also sufficient is evident since a rational prime possesses no factor other than itself and units, and the only integers having this type of norm are of the form $\omega + p\bar{\omega}$ or $p\omega + \bar{\omega}$, which is of the form of the primes we considered above.

Thus we see that any rational prime may be factored into two j-primes, these being the two primes which have p as their norms. Thus p may be written as $(p\omega + \bar{\omega})(\omega + p\bar{\omega})$, the only two primes which, except for

associates, possess p as norm.

Also composite integers of F(j), are very simply factored, for if we consider $a\omega + b\bar{\omega}$ where $a = pq$ and $b = rs$ then $a\omega+b\bar{\omega} = (p\omega+r\bar{\omega})(q\omega+s\bar{\omega}$ and since the cross product terms clear out, we can carry out this process in general by factoring each of the parts as above and then forming the factors. By a slight generalization of this process we shall be enabled to establish a unique factorization theorem for F(j). As an example of this we may consider the following:-

Factorize $10\omega + 18\bar{\omega}$. Now $10 = 5x2$ and $18 = 2x3x3$ whence we have the essentially unique factorization as

$$10\omega + 18\bar{\omega} = (5\omega + 2\bar{\omega})(2\omega + 3\bar{\omega})(\omega + 3\bar{\omega}).$$

9. UNIQUE FACTORIZATION THEOREM FOR F(j).

We shall first establish the existence of a division algorithm, that is, a process such that $\alpha = \sigma\beta + \rho$ where $n(\sigma) \neq 0$, $n(\alpha) \neq 0$ and $|n(\rho)| < |n(\beta)| \neq 0$, and then proceed to derive a Euclidian algorithm or a process of determining the greatest common divisor of two integers of F(j), and finally establish a unique factorization theorem.

In the subsequent discussion we shall employ the term 'regular' hyperbolic integer to denote the fact that an integer is neither zero nor a divisor of zero. If therefore, $\alpha = a_1\omega + a_2\bar{\omega}$ and $\beta = b_1\omega + b_2\bar{\omega}$ are any two regular hyperbolic integers we may prove the following,

Theorem 7 :- A necessary and sufficient condition that β/α is that b_1/a_1 and b_2/a_2

Proof :- We may write $\alpha/\beta = \dfrac{a_1\omega + a_2\bar{\omega}}{b_1\omega + b_2\bar{\omega}} = \dfrac{a_1}{b_1}\omega + \dfrac{a_2}{b_2}\bar{\omega}$, so that if b_1/a_1 and b_2/a_2, then it is clear that β/α. Conversely if b_1/a_1, then $a_1 = c_1b_1$, and if b_2/a_2, then $a_2 = c_2b_2$; therefore

$\alpha = a_1\omega + a_2\bar{\omega} = (c_1b_1\omega + c_2b_2\bar{\omega}) = (c_1\omega + c_2\bar{\omega})(b_1\omega + b_2\bar{\omega}) = \beta\gamma$ where $\gamma = c_1\omega + c_2\bar{\omega}$. Therefore β / α by our previous theorem on divisibility.

We now proceed to establish the existence of a division algorithm for F(j), in the following:-

Theorem 8 :- There exist two regular hyperbolic integers, ρ and σ such that

$$(1)\quad \alpha = \sigma\beta + \rho$$

$$(2)\quad 0 < |n(\rho)| < |n(\beta)|$$

Proof:- If $b_1 \nmid a_1$, $b_2 \nmid a_2$, we have by the division algorithm for real numbers that $a_1 = s_1b_1 + r_1$ and $a_2 = s_2b_2 + r_2$

where $0 < r_1 < b_1$ and $0 < r_2 < b_2$.

Choosing $\sigma = s_1\omega + s_2\bar{\omega}$ and $\rho = r_1\omega + r_2\bar{\omega}$

we clearly have the conditions (1) and (2) satisfied.

If however, $b_1 \nmid a_1$, but b_2 / a_2 , we have $a_1 = s_1b_1 + r_1$ and $a_2 = s'b_2 \pm b_2$; $0 < r_1 < b_1$ where $s' = s_2 - 1$ or $s_2 + 1$ according as s_2 is not or is unity and the + or − sign.

So that $s' \pm 1 = s_2$. Therefore choosing

$$\sigma = s_1\omega + s'\bar{\omega}; \rho = r_1\omega + b_2\bar{\omega} ,$$

we have the condition satisfied.

The case b_1 / a_1 , $b_2 \nmid a_2$ can obviously be treated similarly and the proof is thus complete.

Following the method of Theorem 8 we have,

$$(1)\quad \begin{cases} \alpha = \sigma\beta + \rho & |n(\rho)| < |n(\beta)| \\ \beta = \sigma_1\rho + \rho_1 & 0 < |n(\rho_1)| < |n(\rho)| \\ \rho = \sigma_2\rho_1 + \rho_2 & 0 < |n(\rho_2)| < |n(\rho_1)| \\ \rho_1 = \sigma_3\rho_2 + \rho_3 & 0 < |n(\rho_3)| < |n(\rho_2)| \\ \cdots\cdots\cdots & \cdots\cdots\cdots \end{cases}$$

$$\ldots \begin{cases} \rho_{t-1} = \sigma_{t+1}\ \rho_t + \rho_{t+1}\ ;\ 0 < |n(\rho_{t+1})| < |n(\rho_t)|. \\ \rho_t \quad = \sigma_{t+2}\ \rho_{t+1} + \rho_{t+2} \quad 0 < |n(\rho_{t+2})| < |n(\rho_{t+1})| \\ \ldots\ldots\ldots\ldots \end{cases}$$

This process can be continued so long as we find no remainder ρ_{i+1} which is a factor of the previous one (i.e. ρ_i). If such a case were never encountered, we should have an infinite sequence of decreasing positive integers $|n(\alpha)|$, $|(n(\rho)|$, $|n(\rho_1)|$ ... . Hence we must eventually reach the equality, say at the $(t+2)^{th}$ step, then

$\rho_t = \sigma_t + 2\ \rho_{t+1}$ where $|n(\rho_{t+2})| = 0$. from equations(1). Thus $\rho_{t+2} = 0$ since divisors of zero are excluded by the nature of the division algorithm. Hence $\rho_{t+1} \mid \rho_t$.

In fact from the first of the above equations (1), every common factor of α and β is a factor of ρ.; from the second we see that every common factor of β and ρ is a factor ρ_1, and so on. Finally we see that every common factor of ρ_{t+1} and ρ_t is a common factor of ρ_{t+1}. Hence every common factor of α and β is a factor of ρ_{t+1}.

On the other hand we see that from the last of the equations (1), every factor of ρ_{t+1} is a factor of ρ_t, and from the preceeding equation, that every common factor of ρ_{t+1} and ρ_t is a factor of ρ_{t-1} and so on. Finally, every common factor of ρ_1 and ρ, is a factor of β, and that every common factor of ρ and β is a factor of α. Hence, every factor of ρ_{t+1} is a common factor of α and β. Since the largest factor of ρ_{t+1} is ρ_{t+1} itself, we have the result,

Theorem 9:- In Euclid's Algorithm (1) the greatest common divisor of α and β is ρ_{t+1}.

This method is purely formal in character and the following shorter method leads most directly to the familiar expression of the greatest common divisor of α and β in the linear form $\lambda\alpha + \mu\beta$. Thus we have;

Theorem 10 :- Corresponding to two regular hyperbolic integers α and β of F(j), there exists another integer δ with the properties

$$(i)\ \delta \mid \alpha \text{ and } \delta \mid \beta$$

$$(ii)\ \delta = \lambda\alpha + \mu\beta$$

for a proper choice of integers λ and μ of F(j), not divisors of zero.

Proof :- Let us consider two hyperbolic integers $\alpha = a_1\omega + a_2\bar{\omega}$, and $\beta = b_1\omega + b_2\bar{\omega}$ and a third integer $\delta = d_1\omega + d_2\bar{\omega}$, such that $d_1 =$ g.c.d. (a_1, b_1), and $d_2 =$ g.c.d. (a_2, b_2), where these two g.c.d.'s are defined as in R, since a_1, a_2, b_1, b_2, are all rational integers. Now δ divides both α and β, as we may see from

$$\frac{\alpha}{\delta} = \frac{a_1\omega + a_2\bar{\omega}}{d_1\omega + d_2\bar{\omega}} = \frac{a_1}{d_1}\omega + \frac{a_2}{d_2}\bar{\omega}$$

and since $d_1 =$ g.c.d. (a_1, b_1), it must divide a_1, and similarly d_2 must divide a_2, so that $\delta \mid \alpha$; a similar argument will show that $\delta \mid \beta$, and any other divisor of α and β is also a divisor of δ. For since $d_1 =$ g.c.d. (a_1, b_1) any divisor of both a_1 and b_1 will divide d_1 by its definition. Also, any common divisor of a_2 and b_2 will divide d_2, and these are the conditions that an integer dividing both α and β should divide δ by Theorem 7. Thus, every divisor of α and β by the same reasoning is seen to be a divisor of δ. So that δ now satisfies the two conditions, (i) it is a divisor of α and β and (ii) every other divisor of α and β is a divisor of δ. Hence, δ must be the greatest common divisor of α and β as calculated above by means of the division algorithm.

In conclusion, we shall show that δ as defined above, may be expressed as a linear expression in α and β, with coefficients λ and μ which are not divisors of zero. For since

$$d_1 = \text{g.c.d. } (a_1, b_1) \quad \text{and} \quad -d_2 = \text{g.c.d. } (a_2, b_2)$$

then $$d_1 = c_1a_1 + e_1b_1 \quad \text{and} \quad d_2 = c_2a_2 + e_2b_2$$

where c_1, c_2, e_1, e_2, are rational integers. Therefore, on multiplication

of d_1 by ω and d_2 by $\bar{\omega}$, we have,

$$d_1\omega + d_2\bar{\omega} = c_1a_1\omega + e_1b_1\omega + c_2a_2\bar{\omega} + e_2b_2\bar{\omega}$$

which may be written in the form;

$$d_1\omega + d_2\bar{\omega} = (c_1\omega + c_2\bar{\omega})(a_1\omega + a_2\bar{\omega}) + (e_1\omega + e_2\bar{\omega})(b_1\omega + b_2\bar{\omega}),$$

since the terms in $\omega\bar{\omega}$ vanish. In terms of hyperbolic integers, this becomes $\delta = \lambda\alpha + \mu\beta$ where λ and μ are regular hyperbolic integers, since c_1, c_2, e_1, e_2, are all definite rational integers.

As an example, we may calculate the g.c.d. of $10\omega + 8\bar{\omega}$ and $25\omega + 22\bar{\omega}$. The g.c.d. of 10 and 25 is 5, and that of 8 and 22 is 2. So that the

$$\text{g.c.d. } (10\omega + 8\bar{\omega},\ 25\omega + 22\bar{\omega}) = 5\omega + 2\bar{\omega}.$$

Now $5 = 25 - 2(10)$ and $2 = 3(8) - 22$, so that

$$5\omega + 2\bar{\omega} = 25\omega - 2(10)\omega + 3(8)\bar{\omega} - 22\bar{\omega}$$

which we may write as,

$$5\omega + 2\bar{\omega} = (\omega - \bar{\omega})(25\omega + 22\bar{\omega}) + (2\omega + 3\bar{\omega})(10\omega + 8\bar{\omega})$$

We demonstrated previously that any integer of the form $p\omega + \bar{\omega}$ or $\omega + p\bar{\omega}$ is a prime in F(j), by showing that it possessed properties analogous to rational primes in so far as it could not be factored into simpler integers. Making use of this property, we now establish a unique factorization theorem for F(j).

Theorem 11 :- Every integer of F(j) can be represented in one and only one way as the product of prime factors (except, of course, for associates).

Proof :- If we consider an integer $\alpha = a_1\omega + a_2\bar{\omega}$, then, according to the corresponding theorem for R, a_1 and a_2, if they are not already primes, can be factored in a unique manner into the product of rational primes; since they are rational integers. So that if,

$$a_1 = p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r} \text{ and } a_2 = q_1^{f_1}q_2^{f_2}\ldots q_s^{f_s}$$

where the p's and q's are rational primes, so that-

$$\alpha = a_1\omega + a_2\bar{\omega} = (p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r})\omega + (q_1^{f_1}q_2^{f_2}\ldots q_s^{f_s})\bar{\omega},$$

since $\omega\bar{\omega}$ is zero, and this may be written as-

$$a_1\omega + a_2\bar{\omega} = (p_1{}^{e_1}\omega + \bar{\omega})\ldots(p_r{}^{e_r}\omega + \bar{\omega})(\omega + q_1{}^{f_1}\bar{\omega})\ldots(\omega + q_s{}^{f_s}\bar{\omega})$$

Therefore,

$$a_1\omega + a_2\bar{\omega} = (p_1\omega + \bar{\omega})^{e_1}\ldots(p_r\omega + \bar{\omega})^{e_r}(\omega + q_1\bar{\omega})^{f_1}\ldots(\omega + q_s\bar{\omega})^{f_s}$$

where each of the factors on the right hand side is a prime by our definition, and thus we have factorized any composite integer of F(j), into primes or powers of primes of F(j), in a unique manner, except obviously for associates, since the factorization of a_1 and a_2 is unique. We note, however, that we must distinguish between primes such as $p\omega + \bar{\omega}$ and $\omega + p\bar{\omega}$ which, although they possess the same norm, must be treated as different in this connection.

10. FACTORIZATION AND REPRESENTATION OF INTEGERS AS THE DIFFERENCE OF SQUARES.

While in the field of ordinary complex numbers only certain rational integers can be represented as the sum of two squares, and hence factorable, every rational prime may be factored in F(j). In fact, it is evident that any rational prime p is the product of $p\omega + \bar{\omega}$ and $\omega + p\bar{\omega}$.

As in K(i), where the number of representations of an integer as the sum of two squares is investigated; here we seek the number of different representations of a positive rational integer as the difference of two squares. This is equivalent to finding the number of different hyperbolic numbers $a_1 + a_2 j$, where a_1 and a_2 are rational integers which possess the given integer as norm. To this end we first establish the -

Theorem 12:- Every odd rational prime may be represented as the difference of two rational integral squares in one and only one way.

Proof:- If a hyperbolic integer $\alpha = a_1 + a_2 j (a_1 > 0,\ a_2 \gtrless 0)$ has p as its norm, then $a_1{}^2 - a_2{}^2 = (a_1 + a_2)(a_1 - a_2) = p$. Thus one factor is p and the other 1. Whence $p = \left(\frac{p+1}{2} + \frac{p-1}{2} j\right) \cdot \left(\frac{p+1}{2} - \frac{p-1}{2} j\right)$. This shows that the factorization of an odd prime p as the product of conjugate hyperbolic integers is (apart from associates) unique.

Furthermore, each $\frac{p+1}{2} \pm \frac{(p-1)}{2} j$ is a prime and the factorization cannot be carried further. In fact, if $\frac{p+1}{2} + \frac{(p-1)}{2} j = \alpha\beta$ where α and β are integers, then $p = n(\alpha).\, n(\beta)$. Thus either $n(\alpha)$ or $n(\beta)$ is $= \pm 1$ and either α or β is a unit. In like manner $\frac{p+1}{2} - \frac{p-1}{2} j$ is a prime.

Further, by this method it may be seen that the rational prime 2 cannot be so represented. For if 2 were the difference of 2 integral squares, viz; $a_1^2 - a_2^2$, one of $a_1 + a_2$ or $a_1 - a_2$ would be odd and the other even; whereas their sum $2a_1$, is even. We proceed to establish the,

Theorem 13 :- The number of representations of p^e (p being an odd prime and $e > 1$) is exactly $e + 1$ but they are not necessarily all distinct.

Proof:- We may write, $p^e = (a_1 + a_2 j)^e (a_1 - a_2 j)^e$, since $(a_1 + a_2 j)(a_1 - a_2 j) = p$. If we further write, $a_1 + a_2 j = \alpha$ and $(a_1 - a_2 j) = \bar{\alpha}$ we have $p^e = (\alpha)^e (\bar{\alpha})^e$. In view of the unique factorization theorem, the only integral factors (apart from associates) of p^e are evidently $\alpha^{e-i} \bar{\alpha}^i$ where $(i = 0, 1, 2 \ldots, e)$.

Therefore, there are exactly $e + 1$ different expressions of p^e in the form $(a_1 + a_2 j)(a_1 - a_2 j)$ and therefore exactly $e + 1$ expressions of p^e in the form $a_1^2 - a_2^2$ where a_1 and a_2 are rational integers. This leads at once to,

Theorem 14:- If a rational integer $m = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_n^{e_n}$ (p's all odd primes) then the total number of distinct representations of m as the differences of squares is $\frac{1}{2}(e_1 + 1)(e_2 + 1)(e_3 + 1)..(e_n + 1) + \varepsilon\,(\frac{1}{2})$ when $\varepsilon = 1$ or 0 according as all the e's are even or at least one e is odd.

Proof:- We may write,

$$p_1^{e_1} = (\alpha)^{e_1 - i} (\bar{\alpha})^i, \quad (i = 0,1,2,\ldots,e_1)$$
$$p_2^{e_2} = (\beta)^{e_2 - j} (\bar{\beta})^j, \quad (j = 0,1,2,\ldots,e_2)$$
$$p_3^{e_3} = (\gamma)^{e_3 - k} (\bar{\gamma})^k, \quad (k = 0,1,2,\ldots,e_3)$$
$$\cdots\cdots\cdots\cdots$$
$$p_n^{e_n} = (\eta)^{e_n - q} (\eta)^q, \quad (q = 0,1,2,\ldots,e_n)$$

where, as before, we have the number of representations of

$$p_1^{e_1} = e_1 + 1, \quad p_2^{e_2} = e_2 + 1, \ldots\ldots \ldots, \quad p_n^{e_n} = e_n + 1$$

and therefore, the total number of expressions of the form $(a_1 + a_2 j)(a_1 - a_2$ obtained in this way are $(e_1 + 1)(e_2 + 1)(e_3 + 1).....(e_n + 1)$, where each will be of the form

$$\overbrace{\alpha\alpha\cdots\alpha}^{e_1 - i}\ \overbrace{\bar{\alpha}\cdots\bar{\alpha}}^{i}\ \overbrace{\beta\beta\cdots\beta}^{e_2 - j}\ \overbrace{\bar{\beta}\cdots\bar{\beta}}^{j}\ \overbrace{\gamma\gamma\cdots\gamma}^{e_3 - k}\ \overbrace{\bar{\gamma}\bar{\gamma}\cdots\bar{\gamma}}^{k}\ \cdots\cdots\ \overbrace{\eta\eta\cdots\eta}^{e_n - q}\ \overbrace{\bar{\eta}\bar{\eta}\cdots\bar{\eta}}^{q}$$

Now a term is its own conjugate, if and only if $i = \frac{e_1}{2}$, $j = \frac{e_2}{2}$, $k = \frac{e_3}{2}$ ... ... , $q = \frac{e_n}{2}$. If $e_1, e_2, e_3, \ldots, e_n$, are all even, then we have $(e_1+1)(e_2+1)(e_3+1).....(e_n+1)$ of the expressions given above; one and only one of which is its own conjugate, the rest appearing in pairs. Therefore, the number of pairs is $\frac{(e_1+1)(e_2+1)(e_3+1).....(e_n+1) - 1}{2}$ and since either one of a pair of conjugates gives the same representation of m as the difference of two integral squares, and these are distinct representations of m. Also the one expression which is its own conjugate gives one representation, therefore the total number of distinct expressions are -

$$\frac{(e_1+1)(e_2+1)(e_3+1)\ \ldots(e_n+1) - 1}{2} + 1$$

$$= \tfrac{1}{2}(e_1+1)(e_2+1)\ \ldots\ (e_n+1) + \tfrac{1}{2}$$

Per contra, if any e is odd, then no term is its own conjugate and therefore the number of pairs, or distinct representations is,

$$\tfrac{1}{2}(e_1+1)(e_2+1)(e_3+1)\ \ldots\ (e_n+1).$$

Thus in all cases the number of distinct representations of $m = p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n}$ (p's all odd primes) is,

$$\tfrac{1}{2}(e_1+1)(e_2+1)\ \ldots\ (e_n+1), + \varepsilon\ \tfrac{1}{2} \text{ where } \varepsilon = 0 \text{ or } 1$$

according as at least one of the e's is odd or the e's are all even.

We now seek the number of representations of 2^e which gives the following,

Theorem 15 :- The number of distinct representations of 2^e as the difference of two integral squares is $\frac{e-1}{2} + \varepsilon\ \frac{1}{2}$ where $\varepsilon = 1$ or 0 according as e is even or odd.

Proof :- Since $2 = \frac{3+j}{2} \cdot \frac{3-j}{2}$, we may write $2^e = \left(\frac{3+j}{2}\right)^e \cdot \left(\frac{3-j}{2}\right)^e$ or again as $\alpha^e \bar{\alpha}^e$, where $\alpha = \frac{3+j}{2}$ and $\bar{\alpha} = \frac{3-j}{2}$, so that $\alpha\bar{\alpha} = 2$. As before, we factor this expression into hyperbolic numbers having 2^e as norm as follows,- $(\alpha)^{e-i}(\bar{\alpha})^i$, where $i = 0,1,2,\ldots,e$. From $\frac{3+j}{2} = 2\omega + \bar{\omega}$, we have

$$\left(\frac{3+j}{2}\right)^n = (2\omega+\bar{\omega})^n = 2^n\omega + \bar{\omega} = 2^n\left(\frac{1+j}{2}\right) + \left(\frac{1-j}{2}\right) = \frac{2^n+1}{2} + \frac{2^n-1}{2}\,j,$$

which is of the form $\frac{a+bj}{2}$, where a and b are odd rational integers. Likewise $\left(\frac{3-j}{2}\right)^n = \frac{2^n+1}{2} - \frac{2^n-1}{2}\,j$. Now if $0 < i < e$, we can write $\alpha^i \bar{\alpha}^{e-i}$ in one of the forms $(\alpha\bar{\alpha})^k \alpha^m$ or $(\alpha\bar{\alpha})^k \bar{\alpha}^m$, where $k \geqslant m$. Hence, each of these may be expressed in the form $2^k\left(\frac{a_1 + a_2 j}{2}\right) = 2^{k-1}(a_1 + a_2 j)$ where a_1 and a_2 are rational integers. We thus have a representation of $2^e = (2^{k-1}a_1)^2 - (2^{k-1}a_2)^2$ for each value of i from 1 to $e-1$ inclusive. Thus, there will be exactly $e-1$ of these, and, following the same argument as before, the number of these representations that are distinct is $\frac{1}{2}(e-1) + \varepsilon\frac{1}{2}$ where $\varepsilon = 1$ or 0 according as e is even or odd.

Combining this with the previous results, we have that the number of distinct representations of $m = p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n} 2^e$ is

$\frac{1}{2}(e_1+1)(e_2+1)\ldots(e_n+1)(e-1) + \varepsilon\frac{1}{2}$; where $\varepsilon = \begin{cases} 0 \text{ if at least one e is odd.} \\ 1 \text{ if all the e's are even.} \end{cases}$

This formula shows immediately the fact that no odd multiple of 2 can be represented as the difference of squares, but every other rational number may be so represented.

11. CONGRUENCES IN F(j).

As in the case of rational integers, if α/β we say that β is congruent to zero, mod α, and write $\beta \equiv 0$, mod α. Similarly, if $\mu/(\alpha-\beta)$, then we say that α is congruent to β, mod μ, and write $\alpha \equiv \beta$, mod μ. This last equation may be written as $\alpha - \beta = K\mu$ where K may or may not be a divisor of zero.

The importance of this statement will become apparent when we consider the transitivity of the congruence relation; α and β may or may not be divisors of zero.

We shall show that all the integers of F(j), fall into classes with respect to a given regular modulus μ, and that we place two integers in the same or different class according as they are, or are not congruent to each other, mod μ. In our development of the theory of congruences, we shall attempt to preserve as many of the corresponding properties of congruences in the field R as possible.

We shall first of all demonstrate that congruence is an equality relation, and finally, that we may perform the elementary arithmetical operations on congruences.

1. Reflexive :- If α be any integer of F(j), then certainly $\alpha \equiv \alpha, \text{mod } \mu$

2. Symmetric :- If α and β be any two integers of F(j), then $\alpha \equiv \beta$, mod μ implies $\alpha - \beta = K\mu$ or $\beta = \alpha - K\mu$ or $\beta \equiv \alpha$, mod μ

3. Transitive :- If α, β and γ are any three integers of F(j), then $\alpha \equiv \beta$, mod μ implies $\alpha = \beta + K_1\mu$; and $\beta \equiv \gamma$, mod μ implies $\beta = \gamma + K_2\mu$ Therefore $\alpha = \gamma + (K_1 - K_2)\mu$ and so $\alpha \equiv \gamma$, mod μ. It is clear that in order to preserve this property we require divisors of zero as coefficients of μ. For example, if our modulus is $3\omega + 2\bar{\omega}$ and

$\alpha = 8\omega - 3\bar{\omega}$, $\beta = 2\omega - \bar{\omega}$, and $\gamma = -\omega - 3\bar{\omega}$, then we have

$\alpha \equiv \beta$, mod $3\omega + 2\bar{\omega}$ as $(\alpha - \beta) = (6\omega - 2\bar{\omega}) = (3\omega + 2\bar{\omega})$.

$(2\omega - \bar{\omega}) \equiv 0$, mod $3\omega + 2\bar{\omega}$.

$\beta \equiv \gamma$, mod $3\omega + 2\bar{\omega}$ as $(\beta - \gamma) = (3\omega + 2\bar{\omega}) = (3\omega + 2\bar{\omega})$.

$(\omega + \bar{\omega}) \equiv 0$, mod $3\omega + 2\bar{\omega}$

but $\alpha \neq \gamma$ if we do not include zero divisirs, since $\alpha - \gamma \equiv 9\omega \equiv 0$, mod $3\omega + 2\bar{\omega}$ Thus in order to have a division of our numbers into classes with respect to a given modulus as in R, we must admit divisors of zero.

We can now also add and multiply congruences for if,

$$\alpha_1 \equiv \beta_1, \text{mod } \mu \text{ then } \alpha_1 = \beta_1 + \kappa_1 \mu$$
$$\alpha_2 \equiv \beta_2, \text{mod } \mu \text{ then } \alpha_2 = \beta_2 + \kappa_2 \mu$$

then we can write down the following:-

$$\alpha_1 + \alpha_2 = \beta_1 + \beta_2 + (k_1 - k_2)\mu \text{ or } \alpha_1 + \alpha_2 \equiv \beta_1 + \beta_2, \text{mod } \mu \quad \text{and}$$
$$\alpha_1 \cdot \alpha_2 = \beta_1 \beta_2 + (\beta_2 k_1 + \beta_1 k_2 + \underset{K_1 K_2 \mu}{\nu})\mu \text{ or } \alpha_1 \alpha_2 = \beta_1 \beta_2, \text{mod } \mu .$$

Thus congruences in F(j) possess all the properties associated with congruences in R and we now prove the important theorem

Theorem 16 :- If μ be any integer of F(j), the number of numbers in a complete residue system, mod μ, is exactly $n(\mu)$.

Proof :- If we write $a_1\omega + a_2\bar{\omega} \equiv b_1\omega + b_2\bar{\omega}$, mod $c_1\omega + c_2\bar{\omega}$, then

$$(a_1 - b_1)\omega + (a_2 - b_2)\bar{\omega} = (x\omega + y\bar{\omega})(c_1\omega + c_2\bar{\omega}) = xc_1\omega + yc_2\bar{\omega} .$$

So that $a_1 - b_1 = xc_1$ or $a_1 \equiv b_1$, mod c_1, and $a_2 - b_2 = yc_2$ or $a_2 \equiv b_2$, mod c_2, that is b_1 ranges over a complete residue system, mod c_1 and b_2 ranges over a complete residue system, mod c_2 so that by taking all possible combinations of these, there will be $c_1 \cdot c_2$ numbers of the form $a_1\omega + a_2\bar{\omega}$ where $a_1 = 0, 1, 2, \ldots c_1 - 1$, and $a_2 = 0, 1, 2, \ldots, c_2 - 1$, giving $c_1 \cdot c_2 = n(\mu)$ integers in a complete residue system, mod μ and these will include zero divisors.

That these $n(\mu)$ residues are all incongruent to each other, mod μ is clear from the following;- Let us suppose that two of them were congruent, mod μ so that $\alpha \equiv \beta$, mod μ, or $(a_1 - b_1)\omega + (a_2 - b_2)\bar{\omega} \equiv 0$, mod $c_1\omega + c_2\bar{\omega}$ and therefore $a_1 - b_1 \equiv 0$, mod c_1, and $a_2 - b_2 \equiv 0$, mod c_2 ; and we have that either $a_1 = b_1$ or $a_1 \equiv b_1$, mod c_1 and similarly for a_2 and b_2; so that no two members of a residue system can be congruent to each other unless they are equal.

In particular, if one member of a residue class be prime to the, modulus , , all the other members of that class are prime to the modulus also.

Analogous to the theory for rational integers, we have the,

Definition :- The set of all integers incongruent to each other with

respect to a given modulus μ, and prime to it, is a reduced residue system, mod μ.

12. THE Φ - FUNCTION IN F(j).

Definition :- As in R, we define $\Phi(\mu)$, where μ is an integer of F(j), as the number of integers in a reduced residue system, mod μ. We shall show that this definition preserves many of the properties possessed by the ϕ-function in R and K(i). We use a capital Φ to distinguish the function in F(j) from that in R, since they are two different quantities as we shall illustrate in the example following the

Theorem 17. There are exactly $\phi(a_1).\phi(a_2)$ integers in a reduced residue system, mod μ, where $\mu = a_1\omega + a_2\bar{\omega}$ and $\phi(a_1)$ and $\phi(a_2)$ mean the same as in R, since a_1 and a_2 are rational integers.

Proof :- Put $\mu = a_1\omega + a_2\bar{\omega}$ where a_1 and a_2 are rational integers, then there are exactly $\phi(a_1)$ integers in a reduced residue system, mod a_1, and $\phi(a_2)$ in a reduced residue system, mod a_2, so that if we consider all possible combinations of these, there will be exactly $\phi(a_1)\phi(a_2)$ integers in a reduced residue system, mod μ. If a_1 and a_2 are relatively prime rational integers, then we can write $\phi(a_1).\phi(a_2) = \phi(a_1.a_2) = \phi(n(\mu))$; and in this case there are $\phi(n(\mu))$ integers in a reduced residue system, mod μ. However, in anycase we can always write $\Phi(\mu) = \phi(a_1)\phi(a_2)$ where $\mu = a_1\omega + a_2\bar{\omega}$. Further we see that the Φ-function for negative integers is evidently the set of all rational integers in a reduced residue system, mod $(-a)$, and is the same as the set of integers of a reduced residue system, mod (a).

Thus the Φ- function for the associates of any integer μ is the same as that for μ itself, and similarly $\Phi(\bar{\mu}) = \Phi(\mu)$.

To see the essential difference between Φ and ϕ we have only to consider any hyperbolic integer, say $7\omega + 7\bar{\omega}$. Here we have

$$\Phi(7\omega + 7\bar{\omega}) = \phi(7)\phi(7) = 6 \times 6 = 36$$

but $\Phi(7\omega + 7\bar{\omega}) = \phi 7(\omega+\bar{\omega}) = \phi(7) = 6$ since $\omega+\bar{\omega}=1$

Thus, in order to employ the theory developed here, we must express every integer of F(j) in the ω and $\bar{\omega}$ form. Hence for a rational integer a, we have $\Phi(a\omega + a\bar{\omega}) = \phi(a).\phi(a)$ and not just $\phi(a)$ as we should expect.

However, to see the analogy between the Φ - function in F(j) and that for K(i), we state and prove the following corollary to the theorem given above, viz -

Corollary :- If $\alpha = \pi_1^{e1}\pi_2^{e2}\ \ldots\ \pi_n^{e_n}$ where the π's are primes in F(j), then $\Phi(\alpha) = n(\alpha)\prod_{i=1}^{n}\left(1 - \frac{1}{n(\pi_i)}\right)$

Proof :- In virtue of the unique factorization theorem, we may write

$$\alpha = \pi_1^{e1}\pi_2^{e2}\ldots\ \pi_n^{e_n} \quad \text{or}$$

$$= (p_1\omega+\bar{\omega})^{e1}(p_2\omega+\bar{\omega})^{e2}\ldots(p_{r-1}\omega+\bar{\omega})^{e_{r-1}}(\omega+p_r\bar{\omega})^{e_r}\ldots\ldots(\omega+p_n\bar{\omega})^{e_n}$$

where $\pi_i = p_i\omega+\bar{\omega}$, $(i=1,2,\cdots;r-1)$; $\pi_j = \omega+p_j\bar{\omega}$, $(j=r,r+1,\cdots;n)$

Therefore we may write

$$\alpha = (p_1^{e1}p_2^{e2}\ldots p_{r-1}^{e_{r-1}})\omega + (p_r^{e_r}\ldots p_n^{e_n})\bar{\omega}$$

By the previous theorem we have

$$\Phi(\alpha) = \phi(p_1^{e1}\ldots p_{r-1}^{e_{r-1}}).\phi(p_r^{e_r}\ldots p_n^{e_n})$$

Since p_1^{e1}, p_2^{e2}, etc. are all relatively prime, this may be written as

$$\Phi(\alpha) = \phi(p_1^{e1})\phi(p_2^{e2})\ldots\phi(p_{r-1}^{e_{r-1}})\phi(p_r^{e_r})\ldots\phi(p_n^{e_n})$$

$$= p_1^{e1}\left(1-\frac{1}{p_1}\right)p_2^{e2}\left(1-\frac{1}{p_2}\right)\ldots p_n^{e_n}\left(1-\frac{1}{p_n}\right)$$

$$= p_1^{e1}p_2^{e2}\ldots p_n^{e_n}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right)$$

Now $n(\alpha) = p_1^{e1}p_2^{e2}\ldots p_n^{e_n}$ and $n(\pi_1) = p_1, \ldots, n(\pi_n) = p_n$, whence

$$\Phi(\alpha) = n(\alpha)\left(1-\frac{1}{n(\pi_1)}\right)\ldots\left(1-\frac{1}{n(\pi_n)}\right)$$

$$= n(\alpha)\prod_{i=1}^{n}\left(1-\frac{1}{n(\pi_i)}\right)$$

Example :- To show that the two processes are equivalent, we may consider the following example,

$$\Phi(12\omega+24\bar{\omega}) = \phi(12).\phi(24) = 4 \times 8 = 32.$$

but $12\omega+24\bar{\omega} = (2\omega+\bar{\omega})^2(3\omega+\bar{\omega})(\omega+2\bar{\omega})^3(\omega+3\bar{\omega})$

therefore $\Phi(12\omega + 24\bar{\omega}) = (12)(24)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$

$= (12)(24)\left(\frac{1}{4}\right)\left(\frac{4}{9}\right) = 32$

Since $\phi(1) = 1$, we note that, as in R, when we are dealing with a prime viz, $p\omega + \bar{\omega}$, every integer in the residue system is of the form $a\omega + \bar{\omega}$, and also belongs to the reduced residue system, mod $(p\omega + \bar{\omega})$, since a in every case is relatively prime to p.

13. THE ANALOGUE FOR F(j) OF FERMAT'S THEOREM.

Before proceeding to the theorem, we require the following,

Definition :- Two hyperbolic integers $\alpha = a_1\omega + a_2\bar{\omega}$ and $\beta = b_1\omega + b_2\bar{\omega}$ are relatively prime to each other if they possess only the factor $\omega + \bar{\omega} = 1$ and its associates in common and no others. For if we consider two hyperbolic integers $\alpha = a_1\omega + a_2\bar{\omega}$ and $\beta = b_1\omega + b_2\bar{\omega}$ where a_1 is prime to b_1 and a_2 is prime to b_2, then $\frac{b_1\omega + b_2\bar{\omega}}{a_1\omega + a_2\bar{\omega}} = \frac{b_1}{a_1}\omega + \frac{b_2}{a_2}\bar{\omega}$. The only common factor of a_1 and b_1 is 1, and similarly for a_2 and b_2, so that the only common factor of α and β is $\omega + \bar{\omega} = 1$ or its associates, which illustrates the definition given above, and is analogous to the condition for rational integers to be relatively prime. It is clear that if the norms of two integers are relatively prime, then the integers themselves are relatively prime. However, the fact that the norms are not relatively prime does not mean that the integers are not relatively prime, since a_1 could be a factor of b_2 so long as it was not a factor of b_1 and similarly for a_2.

Now we proceed to establish a theorem analogous to the generalized Fermat Theorem for rational integers for those of F(j), but the method will differ since we must take into account the failure of the cancellation law for zero divisors.

Theorem 18:- If μ be any regular integer of F(j), and α any integer relatively prime to μ, then $\alpha^{\Phi(\mu)} \equiv 1, \text{mod}\,\mu$.

Proof:- Choose $\mu = b_1\omega + b_2\bar{\omega}$ and $\alpha = a_1\omega + a_2\bar{\omega}$ where α is a

member of the reduced residue system, mod μ, so that a_1 is prime to b_1 and a_2 is prime to b_2. Now

$$\alpha^{\Phi(\mu)} = (a_1\omega + a_2\bar{\omega})^{\Phi(\mu)} = (a_1\omega + a_2\bar{\omega})^{\phi(b_1)\phi(b_2)}$$
$$= \left[(a_1)^{\phi(b_1)}\right]^{\phi(b_2)}\omega + \left[(a_2)^{\phi(b_2)}\right]^{\phi(b_1)}\bar{\omega}$$

But by Fermat's Theorem for R, since a_1 is prime to b_1, then $a_1^{\phi(b_1)} \equiv 1, \text{mod } b_1$ so that $(a_1)^{\phi(b_1).\phi(b_2)} = \left[(a_1)^{\phi(b_1)}\right]^{\phi(b_2)} \equiv 1, \text{mod } b_1$ and similarly, since a_2 is prime to be b_2 we have $a_2^{\phi(b_2)} \equiv 1, \text{mod } b_2$, so that

$$(a_2)^{\phi(b_2).\phi(b_1)} = \left[(a_2)^{\phi(b_2)}\right]^{\phi(b_1)} = 1, \text{mod } b_2.$$

Thus we have $(a_1\omega + a_2\bar{\omega})^{\Phi(\mu)} \equiv (\omega + \bar{\omega}), \text{mod } (\mu)$ but $\omega + \bar{\omega} = 1$, therefore $(a_1\omega + a_2\bar{\omega})^{\Phi(\mu)} \equiv 1, \text{mod } \mu$.

Example:- Let $\mu = 3\omega + 2\bar{\omega}$ so that a complete residue system is as follows $0, \omega, 2\omega, \bar{\omega}, \omega+\bar{\omega}$, and $2\omega+\bar{\omega}$. The elements of a reduced residue system are clearly $\omega+\bar{\omega}$, and $2\omega+\bar{\omega}$ by definition. The number of these is $2 = \phi(3)\phi(2)$. The total number of residues is $6 = n(\mu) = 3 \times 2$ as it should be. Also

$$(\omega+\bar{\omega})^{\Phi(\mu)} = (\omega+\bar{\omega})^2 \equiv (\omega+\bar{\omega}), \text{mod } 3\omega+2\bar{\omega} \equiv 1. \text{mod } \mu$$
$$(2\omega+\bar{\omega})^{\Phi(\mu)} = (2\omega+\bar{\omega})^2 \equiv (4\omega+\bar{\omega}), \text{mod } \mu \equiv 1, \text{mod } \mu.$$

14. PRIMITIVE ROOTS OF CONGRUENCES.

Definition:- As in R, we say that an integer in a reduced residue system, mod μ, is a primitive root of a congruence, mod μ if $\Phi(\mu)$ is the least exponent for which it is true that $a^{\Phi(\mu)} \equiv \omega+\bar{\omega} \equiv 1, \text{mod } \mu$. That not every member of a reduced residue system, mod μ is a primitive root is obvious from the following, - $\omega+\bar{\omega}$ is a member of a reduced residue system, mod $3\omega+2\bar{\omega}$ but

$\omega+\bar{\omega} \equiv 1$, mod $3\omega+2\bar{\omega}$, but $\Phi(3\omega+2\bar{\omega}) = 2$ so that $\omega+\bar{\omega}$ is not a primitive root of $3\omega+2\bar{\omega}$, since its first power is congruent to 1, mod μ.

Theorem 19 :- A necessary condition that $a_1\omega + a_2\bar{\omega}$ should be a

primitive root of $b_1\omega + b_2\bar{\omega}$ is that a_1 be a primitive root of b_1 and a_2 a primitive root of b_2.

Proof :- By the definition of a primitive root $a_1^{\phi(b_1)} \equiv 1, \text{mod } b_1$ is the equation satisfied by a_1 and $\phi(b_1)$ is the least power for which this is true. Similarly $a_2^{\phi(b_2)} \equiv 1, \text{mod } b_2$. But $\Phi(b_1\omega + b_2\bar{\omega}) = \phi(b_1)\phi(b_2)$. So that if a_1 is a primitive root of b_1 and a_2 a primitive root of b_2, then

$$(a_1\omega + a_2\bar{\omega})^{\phi(b_1)\phi(b_2)} = (a_1)^{\phi(b_1)\phi(b_2)}\omega + (a_2)^{\phi(b_2)\phi(b_1)}\bar{\omega}$$
$$\equiv 1, \text{mod } (b_1\omega + b_2\bar{\omega}).$$

This condition is only necessary, but the following theorem gives the sufficiency condition.

Theorem 20. A sufficient condition that $a_1\omega + a_2\bar{\omega}$ should be a primitive root of $b_1\omega + b_2\bar{\omega}$ is that g.c.d. $(\phi(b_1), \phi(b_2)) = 1$.

Proof :- Let us consider the case where $\phi(b_1)$ and $\phi(b_2)$ are not prime to each other, so that they possess an l.c.m., say c.

Then $c = c_1\phi(b_1)$ and $c = c_2\phi(b_2)$ So that

$$(a_1\omega + a_2\bar{\omega})^c = (a_1)^c\omega + (a_2)^c\bar{\omega} = a_1^{c_1\phi(b_1)}\omega + a_2^{c_2\phi(b_2)}\bar{\omega}$$

which is congruent to $1, \text{mod } (b_1\omega + b_2\bar{\omega})$ but $c < \phi(b_1).\phi(b_2)$, therefore $a_1\omega + a_2\bar{\omega}$ is not a primitive root of $b_1\omega + b_2\bar{\omega}$.

Hence a necessary and sufficient condition that a hyperbolic integer $b_1\omega + b_2\bar{\omega}$ should possess a primitive root $a_1\omega + a_2\bar{\omega}$ is that a_1 should be prime to b_1 and a_2 prime to b_2 and that $\phi(b_1)$, $\phi(b_2)$ are co-prime. (In order for a number to possess a primitive root at all, it must be of the form $a2^n\omega + b2^m\bar{\omega}$ (a,b odd integers) just as we have for R).

15. QUADRATIC RESIDUES AND REMARKS ABOUT QUADRATIC RECIPROCITY.

With respect to a given hyperbolic integer μ, all the integers are divided into three sets. The first set is composed of all the integers not relatively prime to μ. The second set is composed of those integers prime to μ, which are residues, mod μ of squares; and are called quadratic residues; that is, integers x satisfying the equation $K^2 \equiv x, \text{ mod } \mu$.

The third set is composed of those integers prime to μ but which are not congruent to squares, mod μ, and are called quadratic non-residues of μ.

Theorem 21. The quadratic residues of an odd prime p coincide with the residues, modulo p, of the even powers of a primitive root r of p; the quadratic non-residue of p coincide with the residues of the odd powers of r.

Proof:- Any quadratic residue k is congruent modulo p to a square x^2 where x is an integer prime to p. Thus $x \equiv r^1$, mod p (this corresponds to the theorem in R that the powers of a primitive root range over a complete residue system, mod p and hence, one of the powers must be congruent to x as stated above). Hence, $k \equiv r^{2i}$, mod p. Conversely every even power of r is a square and hence congruent to a quadratic residue of p.

Also by a theorem true for R, $r^s \equiv r^t$, mod p if and only if $s \equiv t$, mod p-1. since p—1 is even we cannot have s odd when t is even. Hence, no odd power of r is congruent, mod p to an even power of r. Thus the residue of the odd powers of r give all the quadratic non-residues of p. As an example of this we may consider the following- let $p = \omega + 5\bar{\omega}$ so that the residues are $0, \omega+\bar{\omega}, \omega+2\bar{\omega}, \omega+3\bar{\omega}, \omega+4\bar{\omega}$, of which $\omega+\bar{\omega}$, and $\omega+4\bar{\omega}$ are the quadratic residues. The only primitive root of $\omega+5\bar{\omega}$ is $\omega+2\bar{\omega}$ the even powers of which correspond to the quadratic residues found above; and the odd powers correspond to the quadratic non-residues as the should.

As in R we can state the following- that an integer R not divisible by p is a quadratic residue if and only if $R^h \equiv 1$, mod p where $h = \frac{1}{2}(p-1)H$; an integer N not divisible by p is a quadratic non-residue of p, if and only if $N^h \equiv 1$, mod p. For example, if we consider any integer $a\omega + b\bar{\omega}$, it will be a quadratic residue of $\omega + p\bar{\omega}$ or $p\omega+\bar{\omega}$ according as b or a is a quadratic residue of p since the second factor in each case is simply congruent to zero.

Legendre's Symbols:- If $\pi = p\omega+\bar{\omega}$ is any prime and if m is any integer not divisible by p, the symbol (m/p) is defined to have a value +1 or -1

according as m is a quadratic residue or non-residue of p, so that using our previous example we have $(\omega+\bar{\omega}\,/\,\omega+5\bar{\omega})=(\omega+4\bar{\omega}/\,\omega+5\bar{\omega})=+1$ and

$$(\omega+2\bar{\omega}\,/\omega+5\,\bar{\omega})=(\omega+3\bar{\omega}\,/\omega+5\bar{\omega})=-1$$

We note that $(m/p)(n/p)=(mn/p)$ as in R and $(m/p)=m^{\frac{1}{2}(p-1)}$, mod p.

We now add a remark concerning a theorem, termed by Gauss, " The Gem of Higher Arithmetic," namely,

Quadratic Reciprocity. Although no formal theorem concerning quadratic reciprocity may be proved for integers F(j), we conclude this paper by some general remarks concerning quadratic reciprocity in F(j).

For if $\omega+p\bar{\omega}$ and $\omega+q\bar{\omega}$ are distinct primes in F(j), then $\omega+p\bar{\omega}$ will or will not be a quadratic residue of $\omega+q\bar{\omega}$ depending on whether or not p is a quadratic residue or non-residue of q and conversely. For if $\omega+p\bar{\omega}$ is a quadratic residue of $\omega+q\bar{\omega}$ then

$$(\omega+a_1\bar{\omega})^2\equiv\omega+p\bar{\omega}\ ,\text{mod}\ \omega+q\bar{\omega}$$

$$\omega+a_1^{\,2}\bar{\omega}=\omega+p\bar{\omega}+b_1\omega+b_2q\bar{\omega}\ .$$

Therefore, by equating ω and $\bar{\omega}$ parts we have $1\equiv 1$, mod 1: $a_1^{\,2}=p+b_2q$. or $a_1^{\,2}\equiv p$, mod q so that p must be a quadratic residue of q and conversely.

So that we may say that the quadratic character of $\omega+p\bar{\omega}$ with respect to $\omega+q\bar{\omega}$ is the same as the quadratic of p with respect to q. That is

$$\left(\frac{\omega+p\bar{\omega}}{\omega+q\bar{\omega}}\right)\left(\frac{\omega+q\bar{\omega}}{\omega+p\bar{\omega}}\right)=\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=1^{\frac{1}{2}(p-1)\,\frac{1}{2}(q-1)}$$

by the theorem for real numbers. This applies only to primes which possess the same form, viz both of the form $\omega+p\bar{\omega}$ or $p\omega+\bar{\omega}$. This is clear from the fact that in the contrary case the Legendre Symbol has then no meaning; that is $\left(\frac{p\omega+\bar{\omega}}{\omega+q\bar{\omega}}\right)$ is neither ± 1 since the prime $\omega+q\bar{\omega}$ could not have a residue of the form $p\omega+\bar{\omega}$ unless $p=1$, and hence $p\omega+\bar{\omega}$ could not be a quadratic residue of $\omega+q\bar{\omega}$ except in the simple case discussed above.

Bibliography :-

1. The Elements of the Theory of Algebraic Numbers, - Reid.

2. Modern Elementry Theory of Numbers, - Dickson.