CONGRUENCES, PRIMITIVE ROOTS, INDICES
FOR THE FIELD $\mathbb{F}(i)$.

by

William Haddock Simons

A Thesis submitted for the Degree of
MASTER OF ARTS
in the Department
of
MATHEMATICS

THE UNIVERSITY OF BRITISH COLUMBIA
April, 1937
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I.</td>
<td>Congruences of condition.</td>
<td>1</td>
</tr>
<tr>
<td>II.</td>
<td>Equivalent congruences.</td>
<td>3</td>
</tr>
<tr>
<td>III.</td>
<td>System of congruences.</td>
<td>3</td>
</tr>
<tr>
<td>IV.</td>
<td>Congruences in one unknown.</td>
<td>5</td>
</tr>
<tr>
<td>V.</td>
<td>Congruence of first degree in one unknown.</td>
<td>5</td>
</tr>
<tr>
<td>VI.</td>
<td>Integer having certain residues.</td>
<td>7</td>
</tr>
<tr>
<td>VII.</td>
<td>Divisibility of one polynomial by another with respect to a prime modulus, common divisors, common multiples.</td>
<td>10</td>
</tr>
<tr>
<td>VIII.</td>
<td>Unit, associated, and primary polynomials.</td>
<td>11</td>
</tr>
<tr>
<td>IX.</td>
<td>Prime polynomials.</td>
<td>12</td>
</tr>
<tr>
<td>X.</td>
<td>Divisibility of polynomials.</td>
<td>14</td>
</tr>
<tr>
<td>XI.</td>
<td>Congruence of two polynomials with respect to a double modulus.</td>
<td>15</td>
</tr>
<tr>
<td>XII.</td>
<td>Unique factorization theorem.</td>
<td>16</td>
</tr>
<tr>
<td>XIII.</td>
<td>Resolution of a polynomial into its prime factors.</td>
<td>21</td>
</tr>
<tr>
<td>XIV.</td>
<td>General congruence of $\kappa$ th degree in one unknown.</td>
<td>22</td>
</tr>
<tr>
<td>XV.</td>
<td>The congruence $\sum \phi(n) l \equiv 0 \mod n$.</td>
<td>24</td>
</tr>
<tr>
<td>XVI.</td>
<td>Analogue to Wilson's theorem in $\mathcal{K}(i)$.</td>
<td>25</td>
</tr>
<tr>
<td>XVII.</td>
<td>Common roots of two congruences.</td>
<td>26</td>
</tr>
<tr>
<td>XVIII.</td>
<td>Multiple roots of a congruence.</td>
<td>26</td>
</tr>
</tbody>
</table>
XIX. Congruences in one unknown with composite moduli.  

XX. Residue of powers.  

XXI. Primitive roots.  

XXII. Indices.  

XXIII. Solution of congruences by means of indices.  

XXIV. Binomial congruences.  

XXV. Primitive roots of a given prime.  

XXVI. The congruence $x^n \equiv b \mod m$.  
In his text, "The Theory of Numbers and Algebraic Numbers", L. H. Reid states, without proof, that certain relations may be proved true in the field \( k(\iota) \) as in the field of rational numbers.\(^1\) It is the purpose of this thesis to investigate this statement and to supply proofs wherever they may differ from those for the field \( k(\iota) \).

Before doing this, however, it will be necessary to collect together certain definitions and results necessary in later developments.

1. **Numbers of** \( k(\iota) \): Any number of \( k(\iota) \) is a rational fractional function of \( \iota \) with rational coefficients. An integer of \( k(\iota) \) is a number of \( k(\iota) \) of the form \( \alpha = a + b \iota \) where \( a \) and \( b \) are rational integers. When \( b = 0 \) we obtain the rational integers which are a sub field of \( k(\iota) \). The number \( a - b \iota \) found by putting \(-\iota\) for \( \iota \) in any number \( \alpha \) is called the conjugate of \( \alpha \) and is denoted by \( \alpha' \). The norm of any number \( \alpha \) is the product of \( \alpha \) and its conjugate \( \alpha' \),

\[
\mathcal{N}[\alpha] = \alpha \alpha' = (a + b \iota)(a - b \iota) = a^2 + b^2,
\]

and is a positive rational number.

The norm of the product of numbers of \( k(\iota) \) is equal to the product of the norms of its factors. Thus

\[
\mathcal{N}[\alpha \beta \gamma \cdots] = \mathcal{N}[\alpha] \mathcal{N}[\beta] \mathcal{N}[\gamma] \cdots.
\]

\(^1\) L. H. Reid, loc. cit., Chapter 5, § 15, p. 190.
II.

2. **Divisibility**: An integer \( \alpha \) of \( \mathbb{F}(i) \) is said to be divisible by an integer \( \beta \) if there exists an integer \( y \) such that \( \alpha = \beta y \).

An integer of \( \mathbb{F}(i) \) which is a divisor of every integer of the field is called a unit of \( \mathbb{F}(i) \). Evidently \( \pm 1 \) are units of \( \mathbb{F}(i) \). If there be any other units then they must divide \( i \) and, conversely, any divisor of \( i \) is a unit. We therefore find that in \( \mathbb{F}(i) \) there are four units, \( \pm 1, \pm i \).

Factorization is unique for integers of \( \mathbb{F}(i) \).

3. **Congruences in \( \mathbb{F}(i) \)**: Two integers \( \alpha, \beta \) of \( \mathbb{F}(i) \) are said to be congruent with respect to the modulus \( \mu \) if their difference is divisible by \( \mu \). We then write

\[
\alpha \equiv \beta \pmod{\mu},
\]

or

\[
\alpha - \beta = k\mu.
\]

The fundamental laws of addition, subtraction, multiplication, and division of congruences apply in the field \( \mathbb{F}(i) \) as in the rational field.

If the integers of \( \mathbb{F}(i) \) are divided into classes, putting two integers in the same or different classes according as they are congruent or incongruent, mod \( \mu \), it may be proved that there are \( \mu [\mu] \) such classes.

The system of integers formed by taking one from each class is called a complete residue system, mod \( \mu \), i.e., the set is such that no two are congruent, mod \( \mu \).
III.

Therefore the $\mathfrak{n} [\mu]$ integers

$$\begin{cases} \mu = 0, 1, \ldots, m(p^e \cdot \xi^{
u}) - 1 \\ \nu = 0, 1, \ldots, m - 1 \end{cases}$$

form a complete residue system, mod $\mu$, where $\mu = m(p^e \cdot \xi^{
u})$.

As special cases we have

(a) When $\mu = p \cdot \xi^{
u}$, $p$ and $\xi$ being rational and prime to each other, the $\mathfrak{n} [\mu]$ integers $1, 2, \ldots, p^e \cdot \xi^{
u}$, form a complete residue system, mod $\mu$.

(b) When $\mu = n$, a rational integer, the $n^2$ integers of $\mathfrak{k}(\kappa)$

$$\begin{cases} \mu = 1, 2, \ldots, |n| - 1 \\ \nu = 1, 2, \ldots, |n| - 1 \end{cases}$$

form a complete residue system, mod $\mu$.

4. The $\phi$-function: As in $\mathbb{R}$, $\phi(\mu)$, where $\mu$ is an integer of $\mathfrak{k}(\kappa)$, is defined as the number of integers in a reduced residue system, mod $\mu$. In later work we will make use of the theorem that if $\delta_1, \delta_2, \ldots, \delta_r$ be the different divisors of $\mu$, then

$$\sum_{\delta} \phi(\delta) = \mathfrak{n} [\mu].$$

We need also Fermat's Theorem, that if $\mu$ be any integer of $\mathfrak{k}(\kappa)$ and $\alpha$ any integer prime to $\mu$, then

$$\alpha^{\phi(\mu)} \equiv 1, \text{ mod } \mu.$$  

Notation. In the work which follows the unknown in the field $\mathfrak{k}(\kappa)$ will be represented by the complex variable, $\zeta$. Integers of the field $\mathfrak{k}(\kappa)$ will be denoted by letters of the Greek alphabet. In particular, the Greek letter, $\pi$, will be used to denote a prime of $\mathfrak{k}(\kappa)$.
I. Congruences of Condition.

In the study of congruences we deal only with relations between definite integers of \( K(\iota) \), a congruence stating that the difference of two integers is divisible by a third integer. In congruences of condition certain of the quantities are unknown and the congruence is true only for particular values of these unknowns.

In the field \( K(\iota) \) we define a polynomial in the undetermined coefficients \( z_1, z_2, \ldots, z_n \) as a rational integral function of \( z_1, z_2, \ldots, z_n \) whose coefficients are rational numbers. In the work which follows, however, the coefficients are integers of the field \( K(\iota) \) unless a statement is made to the contrary.

A polynomial, \( f(z_1, z_2, \ldots, z_n) \) is said to be identically congruent to zero, mod \( \mu \), if all its coefficients are congruent to zero, mod \( \mu \), i.e.,
\[
f(z_1, z_2, \ldots, z_n) \equiv 0 \pmod{\mu}
\]
if
\[
\alpha_i \equiv 0 \pmod{\mu}, \quad (i = 1, 2, \ldots, n)
\]
where the \( \alpha_i \) is the coefficient of \( z_i \) in \( f(z_1, \ldots, z_n) \). Two polynomials \( f(z_1, \ldots, z_n), \varphi(z_1, \ldots, z_n) \) are identically congruent to each other, mod \( \mu \), if their difference is identically congruent to zero mod \( \mu \).

1. \( \equiv \) is the symbol for "identically congruent to" while \( \equiv \) is the symbol for "congruent to" and is used when the congruence expresses a relation between definite integers.
This implies that the coefficients of \( g_i \) in \( f(z_1, \ldots, z_n) \) and \( \varphi(z_1, \ldots, z_n) \) must be congruent, mod \( \mu \).

If \( f(z_1, \ldots, z_n) \equiv \varphi(z_1, \ldots, z_n), \mod \mu \), and \( \alpha_1, \ldots, \alpha_n \) be any \( n \) integers of \( \mathbb{Z} \) then

\[
\tag{1}
f(\alpha_1, \ldots, \alpha_n) \equiv \varphi(\alpha_1, \ldots, \alpha_n), \mod \mu.
\]

That \( z_1, \ldots, z_n \) shall have a set of values such that (1) holds is expressed by

\[
\tag{2}
f(z_1, \ldots, z_n) \equiv \varphi(z_1, \ldots, z_n), \mod \mu
\]

and is called a congruence of condition, and any set of integers \( \alpha_1, \ldots, \alpha_n \) such that (1) is true is called a solution of (2).

If \( \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \) be two sets of solutions such that \( \alpha_i \equiv \beta_i, \mod \mu \) \( (i = 1, \ldots, n) \) then evidently

\[
\tag{3}
f(\alpha_1, \ldots, \alpha_n) \equiv f(\beta_1, \ldots, \beta_n), \mod \mu
\]

and

\[
\varphi(\alpha_1, \ldots, \alpha_n) \equiv \varphi(\beta_1, \ldots, \beta_n), \mod \mu
\]

and hence if \( \alpha_1, \ldots, \alpha_n \) is a solution of (2) then \( \beta_1, \ldots, \beta_n \) is also a solution. These, however, are looked upon as identical. In order that two solutions may be considered as distinct it is necessary that at least one value of one unknown shall be incongruent to the corresponding value of the unknowns in the second solution. Hence in order to find the solutions of any congruence of condition it is sufficient to substitute for the unknowns the \( n[\mu] \) values of a complete residue system, mod \( \mu \).
II. Equivalent Congruences.

Two congruences
\[ f_j(z_1, \cdots, z_n) \equiv g_j(z_1, \cdots, z_n) \mod \mu \quad (1) \]
and
\[ f_j(z_1, \cdots, z_n) \equiv g_j(z_1, \cdots, z_n) \mod \mu \quad (2) \]
are said to be equivalent if every solution of the first is a solution of the second, and if every solution of the second is a solution of the first. Thus, we may add to (1), term by term, the terms of any identical congruence, thus obtaining a congruence equivalent to (1). By means of this we may transpose all terms from one side of a congruence to the other side obtaining an equivalent congruence of the form
\[ \chi(z_1, \cdots, z_n) \equiv 0 \mod \mu. \]
We may also reduce the coefficients of the terms of the polynomial to their smallest absolute values, mod \( \mu \).
Also, we may multiply or divide both members of a congruence by an integer prime to the modulus and obtain an equivalent congruence.

III. System of Congruences, Equivalent Systems.

Instead of a single congruence, we may have a system of congruences in \( z_1, \cdots, z_n \)
\[ f_i(z_1, \cdots, z_n) \equiv 0 \mod \mu_i \quad (i = 1, \cdots, m) \]
and require that these be satisfied simultaneously for values of \( z_1, \cdots, z_n \).
By a solution of such a system of congruences we mean a set of values \( z_1, \cdots, z_n \) which satisfy all the congruences
of the system simultaneously. Two solutions \( \alpha_1, \ldots, \alpha_n \)
and \( \beta_1, \ldots, \beta_n \) are considered different when and only when
the \( m \times n \) congruences
\[
L_i \equiv \beta_i \pmod{y_j} \quad (j = 1, \ldots, m)
\]
are not all true simultaneously.

Two systems of congruences are said to be equivalent when
each solution of the first system is a solution of the
second and each solution of the second is a solution of
the first.

Example: Solve the system of congruences,
\[
(3+2i) x + (2-i) y + 4i z = 1 + 3i, \quad \text{mod } 2 + 5i
\]
\[
(1-i) x + 3 y - (2+3i) z = 1 + i, \quad \text{mod } 2 + 5i
\]
\[
x - (1-2i) y + (2-3i) z = 1 + 4i, \quad \text{mod } 2 + 5i
\]

(a)

Multiply the 3rd congruence by \( 3+2i \), then by \( 1-i \) and
subtract from the 1st and 2nd respectively. Then
\[
(3+3i) y + (12-3i) z = -3+7i, \quad \text{mod } 2 + 5i
\]
\[
(1-3i) y - z = -1-2i, \quad \text{mod } 2 + 5i
\]
\[
x - (1-2i) y + (2-3i) z = 1 + 4i, \quad \text{mod } 2 + 5i
\]

(b)

Multiply the 2nd congruence by \( 12-3i \) and add to the 1st.

Then
\[
-10i y \equiv -2, \quad \text{mod } 2 + 5i
\]
\[
\frac{1}{2} x - z = 1 - 2i, \quad \text{mod } 2 + 5i
\]
\[
x - (1-2i) y + (2-3i) z = 1 + 4i, \quad \text{mod } 2 + 5i
\]

(c)

The 1st congruence of (b) has one and but one solution

\[
y \equiv 19i \equiv -(8+2i), \quad \text{mod } 2 + 5i
\]

Then from the 2nd congruence of (b)

\[
y \equiv -25+19i \equiv -2i, \quad \text{mod } 2 + 5i
\]

and from the 3rd congruence of (a) we find

\[
x \equiv 25i \equiv -10, \quad \text{mod } 2 + 5i
\]

The solution of (a) then is
\[ x = -10 \]
\[ y = -(8+i) \]
\[ z = -3i \]

IV. Congruences in One Unknown.

The general congruence is one unknown is

\[ f(z) = \alpha_0 + \alpha_1 z + \cdots + \alpha_n z^n \equiv 0, \quad \text{mod } \mu \]

where \( \alpha_0, \ldots, \alpha_n \) are integers of \( \mathbb{Z} \).

If \( \beta \) be any integer of \( \mathbb{Z} \) such that

\[ f(\beta) \equiv 0, \quad \text{mod } \mu \]

then \( \beta \) is called a solution of (1).

The degree of (1) is the degree of the term of highest degree whose coefficient is \( \neq 0 \), mod \( \mu \). In order to find a solution for such a congruence it is only necessary to substitute for the unknown in the equation the numbers of a complete residue system, mod \( \mu \), and find which ones satisfy the condition of the congruence.

V. Congruences of the First Degree in One Unknown.

The general congruence of first degree in one unknown may be written in the form

\[ \alpha z \equiv \beta, \quad \text{mod } \mu \]

where \( \alpha, \beta, \mu \) are integers of \( \mathbb{Z} \).

Theorem 1. The congruence,

\[ \alpha z \equiv \beta, \quad \text{mod } \mu \]

where \( \alpha \) is prime to \( \mu \) has one, and only one solution. Substitute for \( z \) in (1) the \( \mathbb{Z}[\mu] \) values of a complete residue system, mod \( \mu \). Then, by \( \S 3 \) of the Intro-
duction we obtain \( \nu [\alpha] \) values which constitute a complete residue system, mod \( \mu \), and hence one and only one of these values can be congruent to \( \beta \), mod \( \mu \).

Fermat's theorem gives a means of obtaining the root of such a congruence, for since

\[ \lambda \equiv P(\mu) \equiv 1, \mod \mu \]

then

\[ \beta \equiv P(\mu) \equiv \beta, \mod \mu \]

Thus \( \beta \equiv P(\mu) - 1 \) is a root of the congruence

\[ \lambda \equiv \beta, \mod \mu \]

where \( \lambda \) is prime to \( \mu \).

Theorem 2. The necessary and sufficient condition for the solvability of the congruence

\[ \lambda \equiv \beta, \mod \mu \]  \hspace{1cm} (1) \]

is that \( \beta \) shall be divisible by the greatest common divisor, \( \delta \) of \( \lambda \) and \( \mu \), and when this condition is fulfilled the congruence has exactly \( \nu [\delta] \) roots.

We shall give a proof similar to that for the rational field. Let \( \lambda = \alpha, \delta \) and \( \mu = \mu, \delta \) so that \( \lambda, \delta \) and \( \mu, \delta \) are prime to each other. Then,

\[ \lambda, \delta \equiv \beta, \mod \mu, \delta \]

i.e.,

\[ \lambda, \delta \equiv \beta + \kappa \mu, \delta \]

Therefore we must have \( \beta \) divisible by \( \delta \).

Put

\[ \beta = \beta, \delta \]

Then

\[ \lambda, \delta \equiv \beta, \mod \mu, \delta \]  \hspace{1cm} (2) \]

Since \( \lambda \) is prime to \( \mu \), (2) has a root. Moreover, all values of \( \delta \) satisfying (2) will also satisfy (1) since
we may pass from (2) to (1) by multiplication by $\delta$. Therefore that $\beta$ be divisible by $\delta$ is a sufficient condition for the solvability of (1). Moreover all roots of (1) satisfy (2) and are therefore of the form $\beta + \kappa \mu$,

where $\beta$ is a root of (2).

Thus in order that we may have two incongruent roots of (1) we must have

\[ \beta + \kappa \mu, \beta + \kappa_2 \mu, \text{ mod } \mu \]

i.e.

\[ \kappa, \mu \neq \kappa_2, \mu, \text{ mod } \mu \]

\[ \kappa \neq \kappa_2, \text{ mod } \delta. \]

Thus if we substitute for $\kappa$ the integers of a reduced residue system, mod $\delta$, which are $\kappa [\delta]$ in number, we obtain all the incongruent roots of (1), mod $\mu$.

VI. Determination of An Integer That Has Certain Residues With Respect to a Given Series of Moduli.

Consider first the case where the required integer must satisfy simultaneously the two conditions

\[ z \equiv \alpha_1, \text{ mod } \mu, \] (1)

\[ z \equiv \alpha_2, \text{ mod } \mu_2, \] (2)

All integers satisfying (1) are of the form

\[ z = \alpha_1 + \eta \mu, \]

where $\eta$ is an integer of $[\delta]$. In order that this may satisfy (2) we must have

\[ \alpha_1 + \mu, \eta \equiv \alpha_2, \text{ mod } \mu_2 \]

or

\[ \mu, \eta \equiv \alpha_2 - \alpha_1, \text{ mod } \mu_2. \] (3)
In order that (3) may be solvable it is necessary and sufficient that \( \delta \) divide \( \alpha_k - \alpha_l \) where \( \delta \) is the greatest common divisor of \( \mu_k \) and \( \mu_l \).

If this requirement be satisfied and \( \xi \) be a root of (3) then every root \( \gamma \) of (3) must satisfy,
\[
\gamma \equiv \xi \mod \frac{\mu_k}{\delta}
\]
i.e.,
\[
\gamma = \xi + \frac{\mu_k}{\delta} \eta,
\]
where \( \eta \) is an integer of \( \mathbb{K}(x) \).

Then all integers satisfying both (1) and (2) are of the form
\[
\gamma = \alpha_1 + \mu_1 \left( \xi + \frac{\mu_k}{\delta} \eta \right) = \alpha_1 + \mu \xi + \frac{\mu_k \mu_1}{\delta} \eta.
\]
And hence
\[
\gamma \equiv \alpha_1 + \mu \xi \mod \frac{\mu_k \mu_1}{\delta} \tag{4}
\]
If \( \gamma_0 \) be any integer satisfying both (1) and (2), all and only those integers satisfy both (1) and (2) which are congruent to \( \gamma_0 \) with respect to the least common multiple of the moduli of (1) and (2).

The general case of \( \pi \) congruences
\[
\gamma \equiv \alpha_i \mod \mu_i \quad (i=1, \ldots, \pi) \tag{5}
\]
may be solved, if a solution exists, by a repeated application of the above. Hence the common solutions, \( \gamma_i \), of (5) are given by
\[
\gamma_i \equiv \gamma_0 \mod \lambda
\]
where \( \gamma_0 \) is an integer \( \mathbb{K}(x) \) satisfying all the congruences and \( \lambda \) is the least common multiple of the moduli, \( \mu_i, \ldots, \mu_\pi \).
Alternate proof for case when the moduli \( \mu_1, \ldots, \mu_m \) are prime to each other.

In this case \( \lambda = \mu_1, \mu_2, \ldots, \mu_m \). For each modulus \( \mu_i \), select a \( \beta_i \) such that
\[
\beta_i = 1, \mod \mu_i, \quad \beta_i = 0, \mod \mu_j \quad (j \neq i).
\]
This is always possible since the second congruence implies
\[
\beta_i = \mu_1, \ldots, \mu_{i-1}, \mu_{i+1}, \ldots, \mu_m \quad K
\]
and we need only determine \( K \) such that
\[
\mu_1, \ldots, \mu_i, \mu_{i+1}, \ldots, \mu_m \quad K = 1, \mod \mu_i
\]
which has a solution since \( \mu_1, \mu_2, \ldots, \mu_m \quad K \) is prime to \( \mu_i \).

Now put
\[
\rho = \sum_{i=1}^{m} \lambda_i \beta_i \quad (6)
\]
Then
\[
z = \rho, \mod \mu_1, \ldots, \mu_m
\]
gives the common solutions of the system. From (6) we also have
\[
z = \rho, \mod \mu_i
\]
and hence since all of \( \beta_1, \ldots, \beta_m \) are divisible by \( \mu_i \) except \( \beta_i \), we have
\[
z = \lambda_i \beta_i, \mod \mu_i
\]
Now
\[
\beta_i = 1, \mod \mu_i
\]
and so
\[
z = \lambda_i, \mod \mu_i
\]
Therefore all integers satisfying (6) satisfy each of the congruences (5). Now let \( z_0 \) be an integer satisfying each of the congruences (5). Then
\[
z_0 = \lambda_i, \mod \mu_i \quad (i = 1, \ldots, m)
\]
and
\[
p = \lambda_i, \mod \mu_i \quad (i = 1, \ldots, m)
\]
Hence
\[
z_0 - p = 0, \mod \mu_i \quad (i = 1, \ldots, m)
\]
i. e. \( \tilde{z}_0 - \rho \) is divisible by each of the moduli \( \mu_1, \ldots, \mu_n \) and hence by their product \( \lambda \). Hence \( \tilde{z}_0 \equiv \rho \, \text{mod} \, \lambda \).

Thus we have a method of obtaining the common solution of a system of congruences in this special case.

If for \( \alpha_1, \alpha_2, \ldots, \alpha_n \) in \( \rho \) we substitute the integers of a complete residue system with respect to the moduli \( \mu_1, \mu_2, \ldots, \mu_n \) respectively, the resulting values of \( \rho \) form a complete residue system, mod \( \lambda \). Or, if for \( \alpha_1, \ldots, \alpha_n \) in \( \rho \) we substitute the integers of reduced residue systems mod \( \mu_1, \mu_2, \ldots, \mu_n \) respectively, the resulting values of \( \rho \) form a reduced residue system, mod \( \lambda \).

The proofs for these two properties are similar to those for the corresponding theorems of \( R \). Hence the number of integers in a reduced residue system, mod \( \mu_1, \mu_2, \ldots, \mu_n \) where \( \mu_1, \ldots, \mu_n \) are prime to each other, is equal to the product of the numbers of the integers in reduced residue systems for each of the moduli \( \mu_1, \ldots, \mu_n \) and therefore

\[
\varphi(\mu_1, \mu_2, \ldots, \mu_n) = \varphi(\mu_1) \varphi(\mu_2) \cdots \varphi(\mu_n).
\]

**VII. Divisibility of One Polynomial by Another With Respect to a Prime Modulus. Common Divisors. Common Multiples.**

Let \( \pi \) be a prime of \( \mathbb{K}(z) \). Then a polynomial \( f(z) \) is said to be divisible by a polynomial \( g(z) \) with respect to the modulus \( \pi \), if there exists a polynomial \( h(z) \) such that

\[
f(z) \equiv g(z)h(z), \quad \text{mod} \, \pi.
\]
As a direct consequence of this definition we have

i. If \( f_1(z) \) be a multiple, mod \( \pi \), of \( f_2(z) \) and \( f_3(z) \) be a multiple, mod \( \pi \), of \( f_3(z) \), then \( f_1(z) \) is a multiple, mod \( \pi \), of \( f_3(z) \); or in general if each polynomial \( f_i(z) \), \( (i=1,2,\cdots) \), be a multiple of \( f_i(z) \), mod \( \pi \), then each polynomial is a multiple, mod \( \pi \), of all that follow it.

ii. If \( f_1(z) \) and \( f_2(z) \) be multiples, mod \( \pi \), of \( f(z) \) then \( f_1(z) + f_2(z) \) and \( f_1(z) - f_2(z) \) are multiples, mod \( \pi \), of \( f(z) \), or in general if \( f_1(z) \) and \( f_2(z) \) be multiples, mod \( \pi \), of \( f(z) \) and \( f_i(z) \), \( f_2(z) \) be any two polynomials, then \( f_1(z)f_1(z) + f_2(z)f_2(z) \) is a multiple of \( f(z) \), mod \( \pi \).

VIII. Unit and Associated Polynomials with Respect to a Prime Modulus, Primary Polynomials.

We wish to find whether there exist polynomials that divide all polynomials with respect to the modulus \( \pi \). No polynomial of degree greater than zero can be such for since they must divide unity, mod \( \pi \), the sum of the degrees of the divisor and quotient would be greater than zero, the degree of unity. Moreover it is evident that they must not be divisible by \( \pi \). Hence, all and only those integers of \( \mathbb{K}(e) \) which are not divisible by \( \pi \) have this property and are called unit polynomials, mod \( \pi \).

Two polynomials which differ only by a unit factor, mod \( \pi \), are called associated polynomials and are looked upon as identical in all questions of divisibility, mod \( \pi \).
If two polynomials $f_1(z), f_2(z)$ are each associated, mod $\pi$, with a third polynomial, they are associated with each other; for if
\[ f_1(z) \equiv \alpha f_3(z), \mod \pi \]
and
\[ f_2(z) \equiv \beta f_3(z), \mod \pi \]
where $\alpha, \beta$, are units, mod $\pi$, and if $\beta'$ is an integer such that
\[ \beta' \beta \equiv 1, \mod \pi, \]
\[ \beta' f_2 \equiv f_3(z), \mod \pi, \]
and then
\[ f_1(z) \equiv \alpha \beta' f_2(z), \mod \pi \]
where $\alpha \beta'$ is a unit, mod $\pi$.

Two polynomials, that are associated, mod $\pi$, are of the same degree, and each is a divisor, mod $\pi$, of the other. Conversely, if two polynomials be each divisible, mod $\pi$, by the other, they are associated.

Two polynomials having no common divisor, mod $\pi$, other than the units are said to be prime to each other, mod $\pi$.

Of the $n[\pi] - 1$ associates of $f(z)$, that one having unity as the coefficient of its term of highest degree is called the "primary associate," mod $\pi$.

IX. Prime Polynomials with Respect to Prime Modulus. Determination of the Prime Polynomials, mod $\pi$, of any Given Degree.

A polynomial that is not a unit, mod $\pi$, and that has no divisors, mod $\pi$, other than its associates and the units, is called a prime polynomial, mod $\pi$. If
it has divisors, mod \( \pi \), other than these it is said to be composite, mod \( \pi \).

For example let us find the primary prime polynomials, mod \( 2+i \), of any degree. We may take as a complete residue system, mod \( 2+i \), the integers \( 0, 1, 2, 3, 4 \), of \( \mathbb{Z}[i] \). Then the primary prime polynomials of the first degree, mod \( 2+i \), are \( z, z+1, z+2, z+3, z+4 \). The reduced primary polynomials of the second degree, mod \( 2+i \), are 25 in number.

\[
\begin{align*}
&z^2, z^2+z, z^2+2z, z^2+3z, z^2+4z \\
&z^2+1, z^2+z+1, z^2+2z+1, z^2+3z+1, z^2+4z+1 \\
&z^2+2, z^2+z+2, z^2+2z+2, z^2+3z+2, z^2+4z+2 \\
&z^2+3, z^2+z+3, z^2+2z+3, z^2+3z+3, z^2+4z+3 \\
&z^2+4, z^2+z+4, z^2+2z+4, z^2+3z+4, z^2+4z+4
\end{align*}
\]

From the primary prime polynomials of the first degree we can form the composite polynomials, mod \( 2+i \). These are

\[
\begin{align*}
&z^2 \equiv z^2 \\
&(z+1)^2 \equiv z^2 + 2z + 1 \\
&(z+2)^2 \equiv z^2 + 4z + 4 \\
&(z+3)^2 \equiv z^2 + 6z + 9 \equiv z^2 + 3z + 6 \\
&(z+4)^2 \equiv z^2 + 8z + 16 \equiv z^2 + 3z + 1 \\
&(z+1)(z+2) \equiv z^2 + 3z + 2 \\
&(z+1)(z+3) \equiv z^2 + 4z + 3 \\
&(z+1)(z+4) \equiv z^2 + 4 \\
&(z+2)(z+3) \equiv z^2 + 3z + 1 \\
&(z+2)(z+4) \equiv z^2 + 3z + 3 \\
&(z+3)(z+4) \equiv z^2 + 2z + 2
\end{align*}
\]

all congruences being taken with respect to the modulus \( 2+i \).
These are 15 in number. The remaining polynomials in (2)
are the primary prime polynomials, mod 2+1 and are 10 in
number.

In general, when \( \kappa > 1 \) the number of primary
prime polynomials, mod \( \pi \), of the \( \kappa \)-degree is

\[
\frac{1}{\kappa} \left[ (\kappa \pi) - \sum (\kappa \pi) \frac{\kappa}{p_1} + \sum (\kappa \pi) \frac{\kappa}{p_1 p_2} + \ldots \right]
\]

where \( p_1, p_2, \ldots \), are the different prime factors of \( \pi \).

X. Division of One Polynomial by Another With Respect
to a Prime Modulus.

Theorem 5. If \( f(z) \) be any polynomial and \( \Phi(z) \) be any
polynomial not identically congruent to zero, mod \( \pi \),
there exists a polynomial \( \mathcal{L}(z) \), such that the polynomial

\[
f(z) - \mathcal{L}(z) \Phi(z) \equiv \mathcal{R}(z), \quad \text{mod } \pi
\]
is of lower degree than \( \Phi(z) \).

The operation of finding \( \mathcal{L}(z) \) and \( \mathcal{R}(z) \) is
called division, mod \( \pi \), of \( f(z) \) by \( \Phi(z) \). \( \mathcal{L}(z) \) is
called the quotient and \( \mathcal{R}(z) \) the remainder in the division,
mod \( \pi \), of \( f(z) \) by \( \Phi(z) \). We prove the existence of \( \mathcal{L}(z) \)
and \( \mathcal{R}(z) \) by giving a method for their determination.

Let

\[
f(z) = \alpha_0 z^m + \alpha_1 z^{m-1} + \ldots + \alpha_m
\]

\[
\Phi(z) = \beta_0 z^m + \beta_1 z^{m-1} + \ldots + \beta_m
\]

be any two polynomials and let

\[
\beta_0 \neq 0, \quad \text{mod } \pi
\]

Consider first the case in which \( \beta_0 = 1 \). Divide \( f(z) \)
by \( \Phi(z) \) as in the ordinary division process until we
get a remainder \( R(z) \) of lower degree than \( \Phi(z) \) and having the quotient \( Q(z) \).

Then:

\[ f(z) = Q(z) \Phi(z) + R(z) \]

from which (1) follows.

Consider the case where \( \beta \neq 1 \) and \( \neq 0 \mod \pi \).

Let \( \tau \) be the reciprocal, \( \mod \pi \), of \( \beta \).

Then:

\[ \tau \Phi(z) \equiv \Phi(z), \mod \pi \]

where \( \Phi(z) \) is a polynomial in \( z \) having unity as the coefficient of the term of highest degree, \( z^\pi \).

Divide \( f(z) \) by \( \Phi(z) \) as before.

Then:

\[ f(z) \equiv Q(z) \Phi(z) + R(z), \mod \pi \]

and hence:

\[ f(z) \equiv \tau Q(z) \Phi(z) + R(z), \mod \pi \]

where \( \tau Q(z) \) and \( R(z) \) are the quotient and remainder required.

XI. Congruence of Two Polynomials With Respect to a Double Modulus.

Two polynomials \( f_1(z) \), \( f_2(z) \) are said to be identically congruent to each other with respect to the double modulus \( \pi \), \( \Phi(z) \), where \( \pi \) is a prime of \( \mathbb{K}(z) \) and \( \Phi(z) \) a polynomial, if their difference, \( f_1(z) - f_2(z) \) is divisible by \( \Phi(z) \mod \pi \).

i.e.

\[ f_1(z) \equiv f_2(z), \mod \pi, \Phi(z) \]

if

\[ f_1(z) - f_2(z) \equiv L(z) \Phi(z), \mod \pi \]

or

\[ f_1(z) - f_2(z) = L(z) \Phi(z) + \pi F(z) \]

where \( L(z) \) and \( F(z) \) are polynomials.

If \( f_1(z) \) is divisible, \( \mod \pi \) by \( \Phi(z) \) this may be
expressed by \( f(z) \equiv 0 \mod \pi, \phi(z) \)

XII. Unique Factorization Theorem for Polynomials With Respect to a Prime Modulus.

In order to prove the unique factorization theorem we need the following theorems.

Theorem 4. If \( f(z) \equiv \phi(z) \phi(z) + R(z) \mod \pi \), every polynomial that divides, mod \( \pi \), both \( f(z) \) and \( \phi(z) \) divides both \( \phi(z) \) and \( R(z) \), and vice versa; that is, the common divisors, mod \( \pi \), of \( f(z) \) and \( \phi(z) \) are identical with the common divisors, mod \( \pi \), of \( \phi(z) \) and \( R(z) \).

This is an immediate consequence of the definition of divisibility.

Theorem 5. If \( f_1(z), f_2(z) \) be any two polynomials and \( \pi \) a prime of \( \mathbb{K}(z) \), there exists a common divisor, \( D(z) \), mod \( \pi \), of \( f_1(z), f_2(z) \) such that \( D(z) \) is divisible, mod \( \pi \), by every common divisor, mod \( \pi \), of \( f_1(z), f_2(z) \), and there exist two polynomials \( \phi_1(z) \) and \( \phi_2(z) \) such that

\[
D(z) \equiv \phi_1(z) \phi(z) + \phi_2(z) \phi_2(z) \mod \pi.
\]

Assume that \( f_2(z) \) is of degree not higher than \( f_1(z) \). Then we may obtain two polynomials \( L(z) \) and \( f_3(z) \) such that

\[
f_1(z) \equiv L(z) f_2(z) + f_3(z) \mod \pi,
\]

\( f_3(z) \) being of lower degree than \( f_2(z) \).
Dividing \( f_2(z) \) by \( f_3(z) \) we obtain
\[
f_2(z) \equiv - \frac{1}{2} f_3(z) f_2(z) + f_1(z), \quad \text{mod } \eta
\]
where \( f_4(z) \) is of degree lower than \( f_3(z) \).

Similarly
\[
f_3(z) \equiv - \frac{1}{2} f_2(z) f_3(z) + f_2(z)
\]
and since the degree of each remainder is decreasing we must finally, after a finite number of steps reach a remainder \( f_{n-1}(z) \) which is zero, mod \( \eta \).

Now the common divisors, mod \( \eta \), of \( f_{n-1}(z) \) and \( f_n(z) \) are identical with those of \( f_{n-2}(z) \) and \( f_{n-1}(z) \), and so on until finally those of \( f_3(z) \) and \( f_2(z) \), with those of \( f_2(z) \) and \( f_1(z) \).

But \( f_n(z) \) is a common divisor, mod \( \eta \), of \( f_{n-1}(z) \) and \( f_n(z) \) and is evidently divisible by every common divisor of \( f_n(z) \) and \( f_{n-1}(z) \). Hence \( f_n(z) \) is the required common divisor, \( D(z) \), mod \( \eta \), of \( f_1(z) \) and \( f_2(z) \).

Now substitute for \( f_3(z) \) in the second congruence its value in terms of \( f_1(z) \) and \( f_2(z) \) found from the first congruence, similarly the values of \( f_3(z) \) and \( f_n(z) \) in the third congruence their values in terms of \( f_1(z) \) and \( f_2(z) \) and continue until the congruence
\[
f_{n-2}(z) \equiv - \frac{1}{2} f_{n-2}(z) f_{n-1}(z) + f_n(z), \quad \text{mod } \eta
\]
where \( f_{n-2}(g) \) and \( f_{n-1}(g) \) are expressed in terms of \( f_1(g) \) and \( f_2(g) \) we shall obtain the congruence
\[
f_1(g) \varphi_1(g) + f_2(g) \varphi_2(g) \equiv \overline{D}(g), \quad \text{mod } \pi
\]

Cor: If \( f_1(g) \), \( f_2(g) \) be two polynomials prime to each other, mod \( \pi \), there exist two polynomials \( \varphi_1(g) \) and \( \varphi_2(g) \) such that
\[
f_1(g) \varphi_1(g) + f_2(g) \varphi_2(g) \equiv 1, \quad \text{mod } \pi
\]

Here \( \overline{D}(g) \) is an integer \( \alpha \), not divisible by \( \pi \), and so we may find two polynomials \( \overline{\varphi}_1(g) \) and \( \overline{\varphi}_2(g) \) such that
\[
f_1(g) \overline{\varphi}_1(g) + f_2(g) \overline{\varphi}_2(g) \equiv \alpha, \quad \text{mod } \pi
\]

Multiplying by the reciprocal, \( \frac{1}{\alpha} \) of \( \alpha \) we have
\[
f_1(g) \varphi_1(g) + f_2(g) \varphi_2(g) \equiv 1, \quad \text{mod } \pi
\]

Theorem 6. If the product of two polynomials \( f_1(g), f_2(g) \), be divisible, mod \( \pi \), by a prime polynomial, \( \overline{P}(g) \), at least one of the polynomials, \( f_1(g), f_2(g) \) is divisible, mod \( \pi \), by \( \overline{P}(g) \).

Let \( f_1(g)f_2(g) \equiv \overline{D}(g) \overline{P}(g), \quad \text{mod } \pi \quad (1) \)

and suppose that \( f_1(g) \) is not divisible, mod \( \pi \), by \( \overline{P}(g) \).

Then there exist two polynomials, \( \varphi_1(g), \varphi_2(g) \) such that
\[
f_1(g) \varphi_1(g) + \overline{P}(g) \varphi_2(g) \equiv 1, \quad \text{mod } \pi
\]
since \( f_1(g) \) and \( \overline{P}(g) \) are prime, mod \( \pi \), to each other.

Then
\[
f_2(g)f_1(g) \varphi_1(g) + f_2(g) \overline{P}(g) \varphi_2(g) \equiv f_2(g), \quad \text{mod } \pi
\]

Hence by (1)
\[
\overline{P}(g)[f_1(g) \varphi_1(g) + f_2(g) \varphi_2(g)] \equiv f_2(g), \quad \text{mod } \pi
\]
where \( \left[ \sum (z) \phi(z) + \sum \phi(z) \right] \) is a polynomial. Hence \( f_2(z) \) is divisible, mod \( \pi \), by \( P(z) \).

Cor 1: If the product of any number of polynomials be divisible, mod \( \pi \), by a prime polynomial \( P(z) \), then at least one of the polynomials is divisible, mod \( \pi \), by \( P(z) \).

Cor 2: If neither of two polynomials be divisible, mod \( \pi \) by a prime polynomial \( P(z) \), their product is not divisible, mod \( \pi \), by \( P(z) \).

Theorem 7. A polynomial \( f(z) \), can be resolved in one and but one way into a product of prime polynomials, mod \( \pi \).

Let \( f(z) \) be a polynomial of degree \( \lambda \), mod \( \pi \) and in its reduced form, mod \( \pi \). Then \( f(z) \) is either prime or has a divisor, \( P(z) \) say, mod \( \pi \). If \( f(z) \) is prime, the theorem is evident. If it is not prime then

\[
 f(z) \equiv P(z) \chi(z), \quad \text{mod} \ \pi
\]

where the sum of the degrees of \( P(z) \), and \( \chi(z) \) is \( \lambda \) and neither is a unit.

If \( P(z) \) is not a prime polynomial it must have a factor \( p(z) \), mod \( \pi \), so that

\[
 P(z) \equiv p(z) \chi(z), \quad \text{mod} \ \pi
\]

where neither \( p(z) \) or \( \chi(z) \) is a unit and the sum of the degrees of \( P(z) \) and \( \chi(z) \) is the same as the degree of \( P(z) \).

If \( P(z) \) is not a prime proceed as before. Since the degrees of the factors are decreasing we must, after a finite number of steps reach a prime polynomial.
20. \( f(z) \equiv P_1(z) f_1(z) \pmod{\pi} \)

Proceed in the same manner with \( f_1(z) \). If it is not prime we must finally obtain

\[ f_1(z) \equiv P_2(z) f_2(z) \pmod{\pi} \]

where \( P_2(z) \) is prime, \( \pmod{\pi} \).

Continuing this process we must after a finite number of factorizations reach a prime polynomial \( P_n(z), \pmod{\pi} \), such that

\[ f(z) \equiv \prod_{i=1}^{n} P_i(z) \pmod{\pi} \]

where \( P_1(z), P_2(z), \ldots, P_n(z) \) are all prime polynomials, \( \pmod{\pi} \), and \( n \) is finite.

To show this factorization is unique, assume that we have

\[ f(z) \equiv \prod_{i=1}^{m} Q_i(z) \pmod{\pi} \]

Then

\[ \prod_{i=1}^{n} P_i(z) \equiv \prod_{j=1}^{m} Q_j(z) \pmod{\pi} \]

Then at least one of the \( Q_j(z) \), say \( Q_1(z) \), must be divisible, \( \pmod{\pi} \), by \( P_1(z) \) and hence, since they are prime, must be associated, \( \pmod{\pi} \)

i.e.

\[ Q_1(z) \equiv \alpha \cdot P_1(z) \pmod{\pi} \]

where \( \alpha \) is a unit, \( \pmod{\pi} \).

Then

\[ \prod_{i=2}^{n} P_i(z) \equiv \prod_{j=2}^{m} Q_j(z) \pmod{\pi} \]
Proceeding as before we may show that for each \( P_i(z) \) there is associated, mod \( \pi \), at least one \( S_j(z) \). Moreover, if two or more \( P_i(z) \)'s are associated with each other at least as many \( S_j(z) \)'s are associated, mod \( \pi \).

In the same manner we may show that with each \( S_j(z) \) there is associated, mod \( \pi \), at least one \( P_i(z) \). Hence the two resolutions are identical except for perhaps a unit polynomial.

Any polynomial may therefore be written in the form

\[
 f(z) \equiv \prod_{j=1}^{\infty} \left[ P_j(z) \right]^{q_j} \mod \pi.
\]

XIII. Resolution of a Polynomial Into Its Prime Factors
With Respect to a Prime Modulus.

The resolution of a polynomial \( f(z) \) into its prime factors, mod \( \pi \), may be effected by dividing, mod \( \pi \), the polynomial by each of the prime polynomials of the first degree \( z, z-1, \ldots, z-\phi(n) \) in turn until one is found which divides \( f(z) \), mod \( \pi \), or it is determined that \( f(z) \) is divisible by none of them, mod \( \pi \).

Let \( z-\alpha \) be the first such polynomial which divides \( f(z) \), mod \( \pi \), and let \( f_1(z) \) be the quotient. Then

\[
 f(z) \equiv (z-\alpha) f_1(z) \mod \pi.
\]

Continuing as before, we see whether \( f_1(z) \) is divisible by any of the remaining prime polynomials of the first
Finally we obtain
\[ f(g) \equiv (g-\alpha_1)(g-\alpha_2)\cdots(g-\alpha_n)f_1(g), \pmod{\mathfrak{p}} \]
where \( f_1(g) \) contains no factors, \( \pmod{\mathfrak{p}} \), of degree less than the second.

To find the prime factors, \( \pmod{\mathfrak{p}} \), of the second degree we determine, in the same manner as above, which prime polynomials of the second degree divide \( f_2(g) \), \( \pmod{\mathfrak{p}} \), and similarly for those of the third degree, etc. If, however, we do not know the prime polynomials of the second degree we may determine whether \( f_2(g) \) is divisible, \( \pmod{\mathfrak{p}} \), by any polynomial of the second degree. If it is, then such a polynomial must be prime since contains no factors of degree less than the second. The same applies for polynomials of higher degree.

**XIV. General Congruence 2nd Degree in One Unknown.**

**Theorem 8.** If \( \rho \) be a root of the congruence
\[ f(g) = \alpha_0 g^n + \alpha_1 g^{n-1} + \cdots + \alpha_n \equiv 0, \pmod{\mathfrak{p}}, \] (1)
then \( f(g) \) is divisible, \( \pmod{\mathfrak{p}} \), by \( g-\rho \), and conversely if \( f(g) \) is divisible, \( \pmod{\mathfrak{p}} \), by \( g-\rho \), then \( \rho \) is a root of (1).

Dividing \( f(g) \) by \( g-\rho \), \( \pmod{\mathfrak{p}} \), we obtain
\[ f(g) \equiv (g-\rho) \varphi(g) + f(\rho), \pmod{\mathfrak{p}} \]
If \( \rho \) is a root of (1) then \( f(\rho) \equiv 0, \pmod{\mathfrak{p}} \).

Hence \( f(g) \equiv (g-\rho) \varphi(g), \pmod{\mathfrak{p}} \)
i.e. \( f(g) \) is divisible, \( \pmod{\mathfrak{p}} \), by \( g-\rho \).
Conversely if \( f(g) \) is divisible by \( g - \rho \mod \pi \), then \( f(\rho) = 0 \mod \pi \), and hence \( \rho \) is a root of (1).

**Theorem 9.** The number of roots of the congruence

\[ f(g) = \lambda_0 g^{n_0} + \cdots + \lambda_n g^n \equiv 0 \mod \pi, \quad \lambda_0 \neq 0 \mod \pi, \]

where \( \pi \) is a prime of \( \mathbb{F}(\epsilon) \), is not greater than its degree.

This follows since \( f(g) \) cannot have more roots than it has linear factors and it cannot have more linear factors than its degree when the modulus is a prime.

**Cor:** If the congruence

\[ f(g) \equiv 0 \mod \pi \]  \hspace{1cm} (1)

has exactly as many roots as its degree and \( \phi(g) \) be a divisor, mod \( \pi \), of \( f(g) \), then the congruence

\[ \phi(g) \equiv 0 \mod \pi \]

has exactly as many roots as its degree.

For since

\[ f(g) = \phi(g) \phi'(g) \mod \pi \]  \hspace{1cm} (2)

then every root of (1) is a root of either

\[ \phi(g) \equiv 0 \mod \pi \]  \hspace{1cm} (3)

or of

\[ \phi'(g) \equiv 0 \mod \pi \]  \hspace{1cm} (4)

Now the sum of the degrees of (3) and (4) is equal to the degree of (1) so that if (3) has fewer roots than its degree, then (4) has more roots than its degree and vice versa, which is contrary to theorem.
XV. The Congruence \( z^{\phi(\mu)} - 1 \equiv 0 \pmod{\mu} \).

Theorem 10. The congruence
\[
\begin{align*}
\sum_{\mu} z^{\phi(\mu)} - 1 & \equiv 0 \pmod{\mu} \\
\text{has exactly as many roots as its degree.}
\end{align*}
\]

By Fermat's theorem we see that the \( \phi(\mu) \) integers of a reduced residue system, mod \( \mu \), satisfy (1). Moreover, since two integers which are congruent, mod \( \mu \), must have with \( \mu \) the same greatest common divisor, any integer satisfying (1) must have with \( \mu \) the greatest common divisor unity, that is, must be prime to \( \mu \). Hence the number of roots of (1) is exactly equal to \( \phi(\mu) \), its degree.

Cor. If \( \sigma \) be a positive divisor of \( \mu \), then the congruence
\[
z^{\sigma - 1} \equiv 0 \pmod{\sigma},
\]
where \( \sigma \) is a prime of \( \mathbb{Z} \), has exactly \( \sigma \) roots; for \( z^{\sigma - 1} \) is a divisor of \( z^{\mu/\sigma - 1} \) and hence by the cor. of theorem 9, the congruence (1) has as many roots as its degree.

When \( \sigma \) is a prime of \( \mathbb{Z} \) the congruence
\[
z^{\frac{\mu}{\sigma}} - z \equiv 0 \pmod{\sigma}
\]
has \( \frac{\mu}{\sigma} \) roots and hence if \( \alpha, \ldots, \alpha_{\frac{\mu}{\sigma}} \) constitute a complete residue system, mod \( \sigma \), we have the identical congruence
\[
z^{\frac{\mu}{\sigma}} - z \equiv (z - \alpha_1)(z - \alpha_2) \cdots (z - \alpha_{\frac{\mu}{\sigma}}) \pmod{\sigma}
\]
or, since \( \sigma \) is a prime, we may choose as our residue
system, mod \( \mathbb{N} \), the \( \mathbb{N} [\pi] \) rational integers

\( 0, 1, 2, \ldots, \mathbb{N} [\pi] - 1 \), and so

\[ z^{\mathbb{N} [\pi]} \equiv z (z-1) (z-2) \ldots (z - \mathbb{N} [\pi] - 1), \mod \pi \]

XVI. Analogue to Wilson's Theorem in \( \mathbb{N} [\pi] \).

If \( \pi \) be a prime of \( \mathbb{N} [\pi] \) and \( \rho, \rho_1, \ldots, \rho(\pi) \)
be a reduced residue system, mod \( \pi \), then

\[ \rho \rho_1 \ldots \rho(\pi) + 1 \equiv 0, \mod \pi. \]

We have

\[ z^{\phi(\pi)} - 1 \equiv (z - \rho) \ldots (z - \rho(\pi)), \mod \pi \quad (1) \]

Let \( S_j \) be the sum of all possible products of \( \rho, \ldots, \rho(\pi) \)
taking \( j \) at a time. Then

\[ z^{\phi(\pi)} = z^{\phi(\pi)} - S_1 z^{\phi(\pi) - 1} + \ldots + (-1)^{\phi(\pi)} S_{\phi(\pi)}, \mod \pi \]

Equate coefficients of like powers of \( z \). Then

\[ S_1 = \rho + \rho_1 + \ldots + \rho(\pi) \equiv 0, \mod \pi \]

\[ S_2 = \rho \rho_1 + \ldots + \rho(\pi) \rho(\pi - 1) \equiv 0, \mod \pi \]

\[ (-1)^{\phi(\pi)} S_{\phi(\pi)} = (-1)^{\phi(\pi)} \rho \rho_1 \ldots \rho(\pi) \equiv -1, \mod \pi \]

Now since \( \mathbb{N} [\pi] = \pi^{-1} \) is always odd except when
\( \pi = 1 + i \) or its associates, \( \phi(\pi) = \mathbb{N} [\pi] - 1 \)
is even and therefore

\[ \rho \rho_1 \ldots \rho(\pi) + 1 \equiv 0, \mod \pi. \]

When \( \pi = 1 + i \), or its associates, \( \mathbb{N} [\pi] = 2 \),
\( \phi(\pi) = 1 \), and we see that the theorem is also satisfied.

The theorem may also be proved directly by
putting \( z = 0 \) in the congruence (1) and proceeding as above.
XVII. Common Roots of Two Congruences.

The common roots of two congruences
\[ f(z) \equiv 0, \quad \text{mod } \pi \]
and
\[ f(z) \equiv 0, \quad \text{mod } \pi \]
are the roots of the congruence
\[ \Phi(z) \equiv 0, \quad \text{mod } \pi \]
where \( \Phi(z) \) is the greatest common divisor, mod \( \pi \), of \( f(z) \) and \( f(z) \).

Therefore, in order to find the incongruent roots of any congruence with prime modulus, we need only find the roots of the congruence
\[ \Phi(z) \equiv 0, \quad \text{mod } \pi \]
where \( \Phi(z) \) is the greatest common divisor, mod \( \pi \), of the given congruence and the congruence
\[ z^{\pi} - z \equiv 0, \quad \text{mod } \pi . \]
This follows since the latter congruence has for its roots the roots of a complete residue system, mod \( \pi \).

XVIII. Determination of Multiple Roots of a Congruence with Prime Modulus.

Theorem 11. If the congruence
\[ f(z) \equiv 0, \quad \text{mod } \pi \]
has a multiple root \( \rho \) of order \( e \), the congruence
\[ f'(z) \equiv 0, \quad \text{mod } \pi \]
has a multiple root \( \rho \) of order \( e - 1 \).

For let \( \Phi(z) \) be a prime polynomial, mod \( \pi \) and suppose \( f(z) \) is divisible, mod \( \pi \), by \( [\Phi(z)]^e \) but not by \( [\Phi(z)]^{e+1} \).
Then
\[ f'(z) = \left[ P(z) \right]^{e-1} \left( P'(z) P(z) + [P(z)]^e L(z) + \pi F'(z) \right). \]
where \( P, P', L, F' \) are polynomials in \( z \).

Therefore
\[ f'(z) \equiv \left[ P(z) \right]^{e-1} L(z), \mod \pi \]

where
\[ L(z) = \epsilon P'(z) P(z) + P(z) L'(z) \]
is a polynomial. Moreover \( L(z) \) is not divisible, \mod \( \pi \), by \( P(z) \) since \( P'(z) \) is of degree less than \( P(z) \) and \( L(z) \) is prime to \( P(z) \), \mod \( \pi \). Therefore \( f'(z) \) is divisible, \mod \( \pi \), by \( \left[ P(z) \right]^{e-1} \) but not by \( \left[ P(z) \right]^e \).

In particular, if \( f(z) \) has a root, \( \rho \), of order \( e \), then \( f'(z) \) has a root, \( \rho \), of order \( e-1 \).

XIX. Congruences in One Unknown and with Composite Moduli.

To find the solution of a congruence of the form
\[ f(z) = \alpha_0 z^n + \alpha_1 z^{n-1} + \cdots + \alpha_n \equiv 0, \mod \mu \]
where \( \mu = \mu_1 \mu_2 \cdots \mu_r \)

Case I. When \( \mu_i \) are integers of \( \mathbb{Z}(\omega) \) which are prime to each other the solution of (1) may be reduced to the
solution of a system of \( t \) congruences

\[ f(x) \equiv 0, \mod e_i \quad (i = 1, \ldots, t) \quad (2) \]

This follows since every root of (1) obviously satisfies each of the congruences (2) while any integer of \( \mathbb{Z}^t \) which satisfies simultaneously the system of congruences (2) must satisfy (1).

If then, \( \beta_i \) be the roots of the congruences (2), and if \( x \) be any integer of \( \mathbb{Z}^t \) such that

\[ x \equiv \beta_i \mod e_i \quad (i = 1, \ldots, t) \quad (3) \]

then \( x \) is a root of the congruence (1).

The system of congruences (3) is always solvable by the method of \( n \sqrt{v} \).

If any one of the congruences (2) has no root, then (1) has no root.

Case II. When \( \mu = \pi_1^{e_1} \pi_2^{e_2} \ldots \pi_r^{e_r} \), the congruence (1) may be solved into the \( r \) congruences

\[ f(x) \equiv 0, \mod \pi_i^{e_i} \quad (i = 1, \ldots, r) \quad (4) \]

The solution of such a congruence may be made to depend upon the solution of one of the form

\[ f(x) \equiv 0, \mod \pi_i^{e_i - 1} \quad (5) \]

where the power of the modulus is one less than in the original congruence, and so finally may be made to depend upon the solution of a congruence of the form

\[ f(x) \equiv 0, \mod \pi_i \]

where \( \pi_i \) is a prime modulus.

For let \( x \) be a root of (5). Then all integers
of the form $\xi + \pi \epsilon^{-\gamma}$ where $\gamma$ is an integer of $\mathbb{K}(\xi)$, are roots of (5). Since all roots of (4) are roots of (5), any root of (4) must be of this form. Then

$$f(\xi + \pi \epsilon^{-\gamma}) \equiv 0, \mod \pi \epsilon^{-\gamma}$$

or

$$f(\xi) + \pi \epsilon^{-\gamma} f'(\xi) \equiv 0, \mod \pi \epsilon^{-\gamma}$$

and hence since $f(\xi) \equiv 0, \mod \pi \epsilon^{-1}$,

$$f(\xi) = K \pi \epsilon^{-1}$$

and dividing each term of (6) by $\pi \epsilon^{-1}$, we find

$$K + f'(\xi) \gamma \equiv 0, \mod \pi \epsilon^{-1}$$

This is a necessary and sufficient condition that $\gamma$ must satisfy in order that a root of (5) may also be a root of (4).

(a) If $f'(\xi) \not\equiv 0, \mod \pi \epsilon^{-1}$, then there is one and but one value of $\gamma$ which will satisfy (7) and so one and but one value $\xi + \pi \epsilon^{-\gamma}$ which satisfies (4).

(b) If $f'(\xi) \equiv 0, \mod \pi \epsilon^{-1}$, and $K \neq 0 \mod \pi \epsilon^{-1}$, there is no value of $\gamma$ satisfying (7), and hence no value of $\xi$ of the form $\xi + \pi \epsilon^{-\gamma}$ satisfying (4); that is, (4) has no root.

(c) If $f'(\xi) \equiv 0, \mod \pi \epsilon^{-1}$, and $K \equiv 0 \mod \pi \epsilon^{-1}$, then (7) is an identical congruence and consequently has $x \lceil \pi \epsilon^{-1} \rceil$ solutions, mod $\pi \epsilon^{-1}$, from which we may find $x \lceil \pi \epsilon^{-1} \rceil$ solutions of (4).
Example: Solve the congruence
\[ 3^3 - (2-3i) z^2 - 4iz + (1+i) = 0, \mod(1-2i). \]  
This may be made to depend upon the solution of
\[ 3^3 - (2-3i) z^2 - 4iz + (1+i) = 0, \mod(1-2i) \]
which has as a root \( z = 1, \mod(1-2i). \)
Then the roots of (1) are of the form
\[ 1 + (1-2i) \xi. \]
Substituting in (1) we obtain
\[ \xi \equiv 0, \mod (1-2i)^2. \]
This gives \( z \) as the only root of (1).

XX. Residue of Powers.

If \( \alpha \) is prime to \( \mu \) and if \( \beta \equiv \alpha^t, \mod \mu \), where \( t \) is a positive rational integer, then \( \beta \) is called a power residue of \( \alpha \) with respect to the modulus \( \mu \).

A system of integers of \( \mathbb{Z} \) such that every power residue of \( \alpha, \mod \mu \), is congruent to one and only one integer of the system, \( \mod \mu \), is called a complete system of power residues of \( \alpha \) with respect to the modulus \( \mu \).

Consider the congruence \( \alpha^t \equiv 1, \mod \mu \) \( (1) \)
It is evident from Fermat's theorem that \( t \) always exists and that \( t \leq \varphi(\mu) \). The integer \( \alpha \) is said to appertain to the exponent \( t \) when \( t \) is the smallest value of \( t \), other than zero, for which the congruence (1) is true.
If \( \alpha \equiv \beta \pmod{\mu} \), then \( \alpha \) and \( \beta \) appertain to the same exponent, \( \pmod{\mu} \).

Theorem 12. If the integer \( \alpha \) appertains to the exponent \( t_\alpha \pmod{\mu} \), then the \( t_\alpha \) powers of \( \alpha \),
\[
\alpha^1, \alpha^2, \ldots, \alpha^{t_\alpha-1}
\]
are incongruent each to each, \( \pmod{\mu} \).

Let \( \alpha^r \) and \( \alpha^s \) be any two of the series (1) and assume that
\[
\alpha^{r+s} \equiv \alpha^s \pmod{\mu}.
\]

Then since \( \alpha \) is prime to \( \mu \),
\[
\alpha^r \equiv 1 \pmod{\mu},
\]
i.e. \( \alpha \) appertains to the power \( r \), \( \mathcal{t}_\alpha \) contrary to the hypothesis that \( \alpha \) appertains to the exponent \( t_\alpha \pmod{\mu} \).

Theorem 13. If \( \alpha \) appertains to the exponent \( t_\alpha \pmod{\mu} \), any two powers of \( \alpha \) with positive exponents are congruent or incongruent to each other, \( \pmod{\mu} \), according as their exponents are congruent or incongruent, \( \pmod{\mu} \).

Let \( \alpha^{s_1}, \alpha^{s_2} \) be any two powers of \( \alpha \) where \( s_1, s_2 \) are positive integers, and let
\[
s_1 = q_1 t_\alpha + r_1, \quad s_2 = q_2 t_\alpha + r_2,
\]
\( q_1 \) and \( q_2 \) being positive integers and
\[
0 \leq r_1 < t_\alpha, \quad 0 \leq r_2 < t_\alpha, \quad r_1 \geq r_2
\]
Assume that
\[
\alpha^{s_1} \equiv \alpha^{s_2} \pmod{\mu},
\]
Then
\[
\alpha^{r_1} \equiv \alpha^{r_2} \pmod{\mu}
\]
and since \( \alpha \) is prime to \( \mu \),
\[ r_i - r_2 \equiv 1, \mod \alpha \]  

But, since \( 0 \leq r_i - r_2 < t_\alpha \) by (2), and \( \alpha \) appertains to the exponent \( t_\alpha \), then

\[ r_i - r_2 = 0 \]

Therefore, from (1)

\[ s_i = s_2, \mod t_\alpha \]  

is a necessary condition for (3) to be true.

Moreover, if (6) is given, then from (1)

\[ r_i = r_2, \mod t_\alpha \]

and hence since \( r_i \) and \( r_2 \) are both less than \( t_\alpha \) we must have

\[ r_i = r_2 \]

Then

\[ \alpha^{r_i} \equiv \alpha^{r_2}, \mod \alpha \]

and since

\[ \alpha^{t_\alpha} \equiv \alpha^{t_\alpha + 1}, \mod \alpha \]

we have

\[ \alpha^{t_\alpha} \equiv \alpha^{t_\alpha + 1}, \mod \alpha \]

Therefore (6) is also a sufficient condition that (3) be true.

Moreover

\[ \alpha^{i t_\alpha + j} \equiv \alpha^{(i+1) t_\alpha + j}, \mod \alpha \]  

\[ (i = 0, 1, 2, \ldots, f - 1; j = 0, 1, \ldots, t_\alpha - 1) \]  

(7)

The relation (7) expresses the law of the periodicity of power residues.
Theorem 14. The exponent $\ell_\alpha$ to which an integer $\alpha$ appertains, mod $\mu$, is a divisor of $\varphi(\mu)$.

For:
$$\varphi(\mu) \equiv 1 \pmod{\ell_\alpha}$$
and, therefore, by theorem 13,
$$\varphi(\mu) \equiv 0 \pmod{\ell_\alpha}$$
i.e. $\varphi(\mu)$ is divisible by $\ell_\alpha$.

Theorem 15. If two integers, $\alpha_1$ and $\alpha_2$, appertain, mod $\mu$, to two exponents $\ell_1$, $\ell_2$, respectively, that are prime to each other, then their product, $\alpha_1 \alpha_2$, appertains, mod $\mu$, to the exponent $\ell_1 \ell_2$.

Let $\alpha_1, \alpha_2$ appertain to the exponent $\ell_1 \ell_2$, mod $\mu$.

Then
$$\left(\alpha_1 \alpha_2\right)^{\ell_1 \ell_2} \equiv 1 \pmod{\mu}$$
and so
$$\ell_1 \ell_2 \equiv 1 \pmod{\mu}$$

But
$$\ell_1 \ell_2 \equiv 1 \pmod{\mu}$$
so that
$$\ell_2 \ell_1 \equiv 1 \pmod{\mu}.$$

But $\alpha_2$ appertains to the exponent $\ell_2$, mod $\mu$, and hence, by theorem 13, $\ell_2 \ell_1 \ell_2$ is divisible by $\ell_2$ and, therefore, since $\ell_1$ and $\ell_2$ are prime to each other, $\ell_1$ is divisible by $\ell_2$. Similarly we may show that $\ell_1$ is divisible by $\ell_2$, so that $\ell_1 \ell_2$ is divisible by $\ell_1 \ell_2$. Hence the smallest value of $\ell$ such that (1) is true is $\ell = \ell_1 \ell_2$. 
Theorem 16. To every positive rational divisor \( t \), or \( \mathcal{P}(\tau) \), there appertain \( \mathcal{P}(\tau) \) integers of \( k(\tau) \) with respect to the modulus \( \tau \), \( \tau \) being a prime of \( k(\tau) \).

Let \( \chi(t) \) denote the number of integers of \( k(\tau) \) which appertain to the exponent \( t \). Then \( \chi(t) \geq 0 \)

Assume that to every positive divisor, \( t \), of \( \mathcal{P}(\tau) \) there appertains at least one integer \( \alpha \). Then each of the integers

\[
\alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^t
\]

which, by theorem 12, are incongruent to each other, mod \( \tau \), is a root of the congruence

\[
\alpha^t \equiv 1, \text{ mod } \tau
\]

For if \( \alpha^r \) be one of them, then

\[
(\alpha^r)^t \equiv (\alpha^t)^r \equiv 1, \text{ mod } \tau
\]

since

\[
\alpha^t \equiv 1, \text{ mod } \tau.
\]

These are, moreover, all the incongruent roots of

(2) since (2) cannot have more roots than its degree, \( \alpha \) being prime to \( \tau \).

Now let \( \alpha^k \) be one of the integers (1) and suppose that \( \alpha^k \) appertains to the exponent \( t \), mod \( \tau \).

Then if \( k \) contains a factor, \( \ell \) say, of \( t \), we have

\[
(\alpha^k)^\ell \equiv (\alpha^t)^\ell \equiv 1, \text{ mod } \tau
\]

and since \( \ell < t \), \( \alpha^k \) does not appertain to the exponent \( t \). Moreover, if \( k \) is prime to \( t \) then \( \alpha^k \) appertains to the exponent \( t \), for suppose \( \alpha^k \) appertains
to the exponent $f$. Then
\[ \alpha^f \equiv 1, \mod \tau, \]
\[ f \equiv 0, \mod \tau, \]
since $\alpha$ appertains to the exponent $\tau$, mod $\pi$.

Therefore
\[ f \equiv 0, \mod \tau \tag{3} \]
since $\kappa$ is prime to $\tau$.

and hence the smallest value of $f$ to satisfy (3) is $f = \tau$.

We have proved, therefore, that the necessary and sufficient conditions that any one of the integers (1) shall appertain to the exponent $\tau$, mod $\pi$, is that its exponent be prime to $\tau$. This is satisfied by $\varphi(\pi)$ of them.

Hence
\[ \chi(\tau) = \varphi(\tau) \text{ or } 0. \]

Since every one of the $\varphi(\pi)$ integers of a reduced residue system, mod $\pi$, appertains to some exponent and every such exponent is a divisor of the $\varphi(\pi)$, it follows that
\[ \sum_{i=1}^{\varphi(\pi)} \chi(t_i) = \varphi(\pi) \]
where $t_i$ are the positive divisors of $\varphi(\pi)$.

But
\[ \sum_{i=1}^{\varphi(\pi)} \varphi(t_i) = \varphi(\pi) \]
whence
\[ \sum_{i=1}^{\varphi(\pi)} \chi(t_i) = \sum_{i=1}^{\varphi(\pi)} \varphi(t_i) \tag{4} \]
If, then, any \( \chi(t_x) = 0 \), (4) would not be true. Hence no \( \chi(t_x) = 0 \) and therefore
\[
\chi(t_x) = \phi(t_x) \quad (x = 1, \ldots, n)
\]

XXI. Primitive Roots.

Any integer that appertains to the exponent \( \phi(n) \) with respect to the modulus \( n \), is said to be a primitive root of \( n \).

If \( \pi \) is a prime of \( \phi(n) \), then by theorem 16, \( \pi \) has \( \phi[\phi(n)] \) incongruent primitive roots. Let \( \rho \) be a primitive root of \( \pi \). Then by theorem 12 the integers \( \rho, \rho^2, \ldots, \rho^{\phi(n)} \) form a reduced residue system, mod \( \pi \). Conversely, if \( \rho, \rho^2, \ldots, \rho^{\phi(n)} \) constitute a reduced residue system, mod \( \pi \), then \( \rho \) is a primitive root. For let \( \rho^a, \rho^b \) be any two of them and let \( a > b > 0 \). Then
\[
\rho^a \equiv \rho^b \mod \pi
\]
i.e.
\[
\rho^{a-b} \not\equiv 1 \mod \pi
\]
where \( a-b \) may have values from 1 to \( \phi(n)-1 \).

In particular
\[
\rho^\phi(n)-1 \not\equiv 1 \mod \pi
\]
But
\[
\rho^\phi(n) \equiv 1 \mod \pi.
\]

Hence \( \rho \) is a primitive root of \( \pi \).

We may therefore define a primitive root of \( \pi \) as an
integer of \( k(i) \) such that a complete system of its power residues, mod \( \nu \), constitute a reduced residue system, mod \( \nu \).

We shall now give a second proof of Wilson's theorem depending upon this definition. Let \( \nu \) be a prime of \( k(i) \) such that \( \nu - 1 \) is odd, and let \( \rho \) be a primitive root of \( \nu \) and \( j_1, \ldots, j_{\phi(\nu)} \) a reduced residue system, mod \( \nu \). Then since \( \rho, \rho^2, \ldots, \rho^{\phi(\nu)} \) also constitute a reduced residue system, mod \( \nu \), we have

\[
\prod_{i=1}^{\phi(\nu)} j_i = \rho^{l_i}, \mod \nu \quad (i = 1, 2, \ldots, \phi(\nu))
\]

and \( l_i \) are the integers 1, 2, \ldots, \( \phi(\nu) \) in some order.  

Multiplying these congruences together we have

\[
\prod_{i=1}^{\phi(\nu)} j_i = \rho^{\sum_{i=1}^{\phi(\nu)} l_i} = \rho^{\sum_{i=1}^{\phi(\nu)} i} , \mod \nu
\]

\[
= \rho^{\frac{\phi(\nu)(1 + \phi(\nu))}{2}}, \mod \nu
\]

But

\[
\rho^{\phi(\nu)} \equiv 1, \mod \nu
\]

\[
\therefore \prod_{i=1}^{\phi(\nu)} j_i \equiv \rho^{\frac{\phi(\nu)}{2}}, \mod \nu
\]

Also

\[
\rho^{\phi(\nu)} = (\rho^{\phi(\nu)/2})^2 \equiv 0, \mod \nu.
\]

But since

\[
\rho^{\frac{\phi(\nu)}{2} - 1} \neq 0, \mod \nu,
\]

we must have

\[
\rho^{\frac{\phi(\nu)}{2} + 1} \equiv 0, \mod \nu.
\]
Therefore \(\prod_{i=1}^{\phi(n)} \phi_i + 1 \equiv 0 \mod n\).

\(\pi[\pi]\) is always odd except when \(\pi = 1 + i\), or its associates, in which case \(\pi[\pi] = 2\). The proof as given here does not apply for this case although the theorem is true since then \(\phi(\pi) = 1\), and we take \(\pi\) as our reduced residue system, \(\mod 1 + i\).

XXII. Indices.

Let \(\rho\) be a primitive root of \(\pi\). Then \(\rho, \rho^2, \ldots, \rho^{\phi(n)}\) constitute a reduced residue system, \(\mod \pi\), so that any number \(\alpha\) which is prime to \(\pi\) must be congruent to some power of \(\rho\), \(\mod \pi\).

If \(\alpha \equiv \rho^i \mod \pi\)

then \(i\) is said to be the index of \(\alpha\) to the base \(\rho\), \(\mod \pi\), and we write

\[i = \text{ind}_\rho \alpha \mod \pi\]

It may be shown that indices obey the following laws analogous to those of logarithms.

1. The index of the product of two integers is congruent to the sum of the indices of the factors, \(\mod \phi(\pi)\)

\[\text{ind}_\rho \alpha \beta \equiv \text{ind}_\rho \alpha + \text{ind}_\rho \beta \mod \phi(\pi)\]

or in general

\[\text{ind}_\rho \alpha_1 \alpha_2 \ldots \equiv \text{ind}_\rho \alpha_1 + \text{ind}_\rho \alpha_2 + \text{ind}_\rho \alpha_3 + \ldots \mod \phi(\pi)\]

Let \(\text{ind}_\rho 1 = i\), \(\text{ind}_\rho \beta = i_2\), \(\text{ind}_\rho \alpha \beta = i\), \(\mod \pi\).
Then
\[ \alpha = \beta^i, \beta = \rho^{i_2}, \alpha \beta = \rho^{i}, \mod \pi \]
and therefore
\[ i_1 + i_2 = i, \mod \phi(\pi) \]
i. e.
\[ \operatorname{ind}_\rho \alpha \beta = \operatorname{ind}_\rho \alpha + \operatorname{ind}_\rho \beta \mod \phi(\pi) \]
As a particular case we have
\[ \operatorname{ind}_\rho \alpha = n \operatorname{ind}_\rho \alpha \mod \phi(\pi) \]
Also
\[ \operatorname{ind}_\rho \frac{\alpha}{\beta} = \operatorname{ind}_\rho \alpha - \operatorname{ind}_\rho \beta \mod \phi(\pi) \]
In every system \[ \operatorname{ind} 1 = 0 \mod \phi(\pi) \]
Now the index of any number depends upon the value of the particular primitive root chosen as base. If, however, the index is known for a particular base we may find its value for any other base.
For let \( \rho_1 \) and \( \rho_2 \) be two primitive roots of \( \pi \), and let
\[ \operatorname{ind}_{\rho_1} \rho_2 = i_1 \mod \pi \]
so that
\[ \rho_2 = \rho_1^{i_1} \mod \pi \]
Let \( \alpha \) be an integer of \( \mathbb{Z}_\pi \) such that
\[ \operatorname{ind}_{\rho_2} \alpha = i_2 \mod \pi \]
Then
\[ \alpha = \rho_2^{i_2} = \rho_1^{i_1} \rho_2^{i_2} \mod \pi \]
and hence
\[ \operatorname{ind}_\rho \alpha = i_1 i_2 = \operatorname{ind}_{\rho_2} \rho_2 \operatorname{ind}_{\rho_2} \alpha \mod \phi(\pi) \]
In particular, putting $\alpha = \beta$, we have

$$\operatorname{ind}_p \beta = \operatorname{ind}_p \beta, \mod \phi(n)$$

i.e.

$$\operatorname{ind}_p \beta \equiv \operatorname{ind}_p \beta, \equiv 1, \mod \phi(n)$$

**Theorem 17.** If $\operatorname{ind}_p \alpha \equiv \beta, \mod n$, be $i$, and $d$ is the greatest common divisor of $i$ and $\phi(n)$, then $\alpha$ appertains to the exponent $\frac{\phi(n)}{d}$.

We are given that $\alpha \equiv \beta, \mod n$.

Let $f$ be the exponent to which $\alpha$ appertains, mod $n$.

We wish to find the least value of $f$ such that

$$2^f \equiv 1, \mod n$$

(1)

Now

$$\alpha^f \equiv 1, \equiv \beta, \mod n$$

and hence

$$\alpha^f \equiv 0, \mod \phi(n)$$

Then

$$f \equiv 0, \mod \frac{\phi(n)}{d}$$

(2)

where $d$ is the greatest common divisor of $i$ and $\phi(n)$.

Then $\frac{i}{d}$ is prime to $\frac{\phi(n)}{d}$ and so the smallest value of $f$, other than zero, such that (2) be satisfied is

$$f = \frac{\phi(n)}{d}$$

Then, by (1), $\alpha$ appertains to the exponent $\frac{\phi(n)}{d}, \mod n$.

The converse of this theorem is also true; i.e., whatever primitive root, $\rho$, of $n$, is taken, if $\alpha$
appertains to the exponent \( \frac{p(n)}{\alpha} \mod q \), then \( d \) is the greatest common divisor of \( \text{ind}_p \alpha \) and \( q(n) \).

Cor: If \( \rho \) is a primitive root of \( q \), then the \( \varphi [q(n)] \) primitive roots of \( q \) are those incongruent powers of \( \rho \) whose exponents are prime to \( q(n) \).

XXIII. Solution of Congruences by Means of Indices.

If we have a table of indices to any base for a given modulus \( q \) we may solve any congruences of the types

(a) \( \alpha z = \beta \mod q \)

or

(b) \( \alpha z^\nu = \beta \mod q \)

where in each case \( \alpha \) is not divisible by \( q \).

In case (a), taking indices, we have

\[ \text{ind } \alpha + \text{ind } z = \text{ind } (\beta, \mod q(n)) \]

whence

\[ \text{ind } z = \text{ind } \beta - \text{ind } \alpha, \mod q(n) \]

and knowing \( \text{ind } \beta \), and \( \text{ind } \alpha \) we may find \( \text{ind } z \) and so find \( z \).

In case (b) we have

\[ \nu \text{ ind } z = \text{ind } \beta - \text{ind } \alpha, \mod q(n) \]

a congruence of the first degree in one unknown. The necessary and sufficient condition that this be solvable is that \( (\text{ind } \beta - \text{ind } \alpha) \) be divisible by \( d \), the greatest common divisor of \( q \) and \( q(n) \). When this condition is satisfied there are \( q(n) [d] \) values of \( \text{ind } z \).
corresponding to which we find \( n \left[ \frac{d}{\lambda} \right] \) values of \( y \) which are incongruent mod \( \pi \) and which satisfy the congruence (b).

XXIV. Binomial Congruences.

We give here another method of treatment for the subject of power residues and primitive roots from a consideration of the binomial congruence

\[ y^{\alpha - 1} \equiv 0 \pmod{\pi} \tag{1} \]

We have seen that all roots of (1) will be roots of the congruence

\[ \varphi(y) \equiv 0 \pmod{\pi} \]

where \( \varphi(y) \) is the greatest common divisor, mod \( \pi \), of \( y^{\alpha - 1} \) and \( y^{\varphi(\pi)} \). It is easily seen that

\[ \varphi(y) = y^{\alpha - 1} \]

where \( \alpha \) is the greatest common divisor of \( \pi \) and \( \varphi(\pi) \).

For all common divisors of \( y^{\alpha - 1} \) and \( y^{\varphi(\pi)} \), must be of the form \( y^{\alpha - 1} \) where \( \alpha \) is a divisor of both \( \pi \) and \( \varphi(\pi) \).

Moreover, if \( \alpha \) is a divisor of \( \pi \), then \( y^{\alpha - 1} \) is a divisor of \( y^{\alpha - 1} \). Hence if \( y^{\alpha - 1} \) is the greatest common divisor of \( y^{\alpha - 1} \) and \( y^{\varphi(\pi)} \), then \( \alpha \) is the greatest common divisor of \( \pi \) and \( \varphi(\pi) \).

The congruence (1) has, therefore, \( d \) incongruent roots and these are the roots of the congruence

\[ y^{d - 1} \equiv 0 \pmod{\pi} \tag{2} \]

Those roots of (2) which satisfy no binomial congruence of degree less than (2) are called primitive
roots of (2) while those roots of (2) which satisfy bi-
nomial congruences of lower degree are called imprimitive
roots.

The primitive roots of (2) are, then, those
integers which appertain to the exponent $d$, mod $\pi$.
They are $\varphi(d)$ in number. In particular, the primitive
roots of $\pi$ are the primitive roots of the congruence
\[ f^{d-1} \equiv 0 \pmod{\pi}. \]

If $\rho$ is a primitive root of (2) then the $d$
roots of (2) are, by theorem 12, $1, \rho, \rho^2, \ldots, \rho^{d-1}$.
If $\alpha_1, \alpha_2$ are roots of the congruences
\[ f^{d-1} \equiv 0 \pmod{\pi} \quad (3) \]
and
\[ f^{d_2-1} \equiv 0 \pmod{\pi} \quad (4) \]
respectively, then $\alpha_1, \alpha_2$ is a root of the congruence
\[ f^{d_1d_2-1} \equiv 0 \pmod{\pi} \quad (5) \]
In particular, if $\alpha_1$ and $\alpha_2$ are primitive roots of (3)
and (4) respectively, and if $d_1$ and $d_2$ are prime to
each other, then $\alpha_1, \alpha_2$ is a primitive root of (5).

XXV. Determination of a Primitive Root of a Given
Prime Number.

The method, due to Gauss, in which we find a
succession of integers appertaining to higher and higher
exponents, will apply equally well in the field $\mathbb{F}$. We must, in such a process, find an integer which appertains
to the exponent $\varphi(\pi)$, mod $\pi$, and hence is a primitive
root of \( \mathfrak{p} \). We may prove, however, that if \( \alpha \) is a primitive root of \( \mathfrak{m} [\mathfrak{p}] \) in \( \mathcal{R} \), then \( \alpha \) is also a primitive root of \( \mathfrak{p} \) in \( \mathcal{K}(i) \).

If \( \alpha \) is a primitive root of \( \mathfrak{m} [\mathfrak{p}] \) in \( \mathcal{R} \), then \( \alpha \) is also a primitive root of \( \mathfrak{p} \) in \( \mathcal{K}(i) \).

Let \( \mathfrak{m} [\mathfrak{p}] = \mathcal{P} \), a rational prime. Then since \( \alpha \) is a primitive root of \( \mathcal{P} \),
\[
\varphi(\mathcal{P}) \equiv 1 \pmod{\mathcal{P}}.
\]
i.e.
\[
\alpha^{\varphi(\mathcal{P})-1} \equiv 1 \pmod{\mathcal{P}}
\]
i.e.
\[
\alpha^{-\varphi(\mathcal{P})-1} \equiv 1 \pmod{\mathcal{P}}
\]
Therefore,
\[
\alpha^{-\varphi(\mathcal{P})-1} \equiv \alpha^{\varphi(\mathcal{P})} \equiv 1 \pmod{\mathcal{P}}.
\]
We must still show that \( \alpha \) does not appertain, mod \( \mathfrak{p} \), to an exponent less than \( \varphi(\mathcal{P}) \). Suppose \( \alpha \) appertains to the exponent \( f \), mod \( \mathfrak{p} \), where \( f < \varphi(\mathcal{P}) \).
Then
\[
\alpha^f \equiv 1 \pmod{\mathcal{P}}
\]
and so, since \( \alpha^f - 1 \) is a rational integer,
\[
\alpha^{f-1} \equiv 1 \pmod{\mathcal{P}}
\]
in which case \( \alpha \) appertains to an exponent \( f, < \varphi(\mathcal{P}) \)
i.e. \( < \varphi(\mathfrak{m} [\mathfrak{p}]) \) in \( \mathcal{R} \), mod \( \mathfrak{m} [\mathfrak{p}] \) and so is not a primitive root of \( \mathfrak{m} [\mathfrak{p}] \), which gives a contradiction. Therefore \( \alpha \) is a primitive root of \( \mathfrak{p} \) in \( \mathcal{K}(i) \).

In order to find a primitive root of \( \mathfrak{p} \), therefore, we need only find a primitive root of \( \mathfrak{m} [\mathfrak{p}] \) in \( \mathcal{R} \). This will also be a primitive root of \( \mathfrak{p} \) in \( \mathcal{K}(i) \).
The remaining primitive roots of \( \mathcal{H} \) may be found by applying the cor. of theorem 17.

For example, to find the primitive roots of \( \mathcal{H} + \mathcal{S} \) first find a primitive root of \( \mathcal{H} \). To do this form the power residues of \( 2 \) \( \mod \mathcal{H} \).

These are
\[
2, 14, 8, 16, 32, 23, 2, 10, 20, -1
\]
\[
-2, -14, -8, -16, -32, -23, -2, -10, -20, +1
\]

Then 2 appertains to the exponent \( 20 \) \( \mod \mathcal{H} \).

Now form the power residues of \( 3 \) \( \mod \mathcal{H} \). We have
\[
3, 9, 27, -1, -3, -9, -27, +1
\]
so 3 appertains to the exponent \( 8 \) \( \mod \mathcal{H} \).

Take
\[
\ell_1 = 20 = 2^2 \times 5
\]
\[
\ell_2 = 8 = 2^3
\]

The greatest common multiple of \( \ell_1 \) and \( \ell_2 \) is \( \mathcal{M} = 40 \).

Divide \( \mathcal{M} \) into two factors \( \mathcal{M}_1 \) and \( \mathcal{M}_2 \) prime to each other and such that \( \mathcal{M}_1 \) is a divisor of \( \ell_1 \) and \( \mathcal{M}_2 \) a divisor of \( \ell_2 \). Then \( \mathcal{M}_1 = 5 \), \( \mathcal{M}_2 = 8 \).

Now
\[
\mathcal{H}_0 = \mathcal{M}, \quad \mathcal{M}_2 = \frac{2^2 \times 5}{2^2 \times 1} = \frac{20}{4} \times \frac{8}{1}
\]

Then 2 and 3 appertain to the exponents \( \frac{20}{4} \) and \( \frac{8}{1} \) respectively and so their product, \( 2^{\frac{20}{4}} \times 3 \), appertains to the exponent \( \frac{20}{4} \times 5 = 10 \). Therefore \( 2^{\frac{20}{4}} \times 3 \) is a primitive root of \( \mathcal{H} \).
Now
\[ 2^4 \times 3 = 18 \equiv 1 \pmod{\mathbb{H}} \]
Therefore \( 7 \) is a primitive root of \( \mathbb{H} \). It is also a primitive root of \( \mathbb{H} = \mathbb{H} + 3 - i \), \( \mathbb{K}(i) \)
Then the \( \phi(\mathbb{H}) = \phi(\mathbb{H}_0) = 16 \) primitive roots of \( \mathbb{H} \) may be found by applying the cor. of theorem 17. That is since \( 7 \) is a primitive root of \( \mathbb{H} + 3 - i \), then the \( \phi(\mathbb{H} + 3 - i) \) primitive roots of \( \mathbb{H} + 3 - i \) are those \( \phi(\mathbb{H} + 3 - i) \) incongruent powers of \( 7 \) whose exponents are prime to \( \phi(\mathbb{H} + 3 - i) \). These are
\[ 7, 7^3, 7^7, 7^9, 7^{23}, 7^{27}, 7^{31}, 7^{37}, \]
which may be reduced to integers of \( \mathbb{K}(i) \).

XXVI. The Congruence \( z^\lambda \equiv \beta \pmod{\mathbb{H}} \)

We may reduce any congruence
\[ \lambda, z^\lambda \equiv \beta, \pmod{\mathbb{H}} \]
where \( \lambda \), is not divisible by \( \mathbb{H} \), to one of the form
\[ z^\lambda \equiv \beta, \pmod{\mathbb{H}} \]
Consider the case in which \( \beta \neq 0, \pmod{\mathbb{H}} \).

From previous discussion we have the theorem,
Theorem 18. The necessary and sufficient conditions that the congruence
\[ z^\lambda \equiv \beta, \pmod{\mathbb{H}} \]
shall be solvable, is that \( \lambda \) and \( \beta \) shall be divisible by the greatest common divisor, \( d \), of \( \lambda \) and \( \phi(\mathbb{H}) \);
this condition being satisfied the congruence has exactly \( \chi[d] \) incongruent roots.

**Theorem 19. Euler's Criterion for the field \( \mathbb{K}(i) \).**

If \( \alpha \) be the positive greatest common divisor of \( \chi \) and \( \varphi(\chi) \), the necessary and sufficient condition that the congruence

\[ \beta^\chi \equiv \beta \pmod{\chi} \]  

shall be solvable is

\[ \beta^{\varphi(\chi)} \equiv 1 \pmod{\chi} \]  

This condition being satisfied, the congruence has exactly \( \chi[d] \) incongruent roots.

Let \( \beta \) be a primitive root of \( \chi \), and let \( \text{ind}_\beta \beta = e \). If (2) is solvable then \( e \) is divisible by \( d \).

Let \( e = md \). Then

\[ \beta^{md} \equiv \beta \pmod{\chi} \]

and

\[ \beta^{\varphi(\chi)} = \beta^{md^{\varphi(\chi)}} \equiv 1 \pmod{\chi} \]

Therefore (3) is a necessary condition for the solvability of (2). Conversely, if \( \beta \) satisfies condition (3), then since

\[ \beta^{md} \equiv \beta \pmod{\chi} \]

then

\[ \beta^{md^{\varphi(\chi)}} \equiv \beta^{\varphi(\chi)} \pmod{\chi} \]

and hence

\[ \beta^{\varphi(\chi)} \equiv 1 \pmod{\chi} \]
and since \( \beta \) is a primitive root,
\[
\frac{\phi(n)}{\alpha} \equiv 0 \pmod{\phi(n)}
\]
so that \( \frac{\epsilon}{\alpha} \) is an integer. Therefore \( \epsilon \) is divisible by \( \alpha \) and (2) is solvable.

Hence (3) is also a sufficient condition for the solvability of (2).

All incongruent integers \( \beta \), for which the congruence (2) is solvable may be obtained by observing that they are roots of the congruence
\[
z \frac{\phi(n)}{\alpha} \equiv 1 \pmod{\phi(n)}
\]
The congruence (4) has \( \frac{\phi(n)}{\alpha} \) incongruent roots which are the incongruent values of \( \beta \) for which (2) is solvable.

Such members congruent to the \( n \)th power of an integer, \( \text{mod} \ n \), are called \( n \)-ic residues of \( n \), and we have the following:

**Theorem 20.** The number of incongruent \( n \)-ic residues, \( \text{mod} \ n \), is \( \frac{\phi(n)}{\alpha} \) where \( \alpha \) is the positive greatest common divisor of \( n \) and \( \phi(n) \) and these residues are roots of the congruence
\[
z \frac{\phi(n)}{\alpha} \equiv 1 \pmod{\phi(n)}.
\]