A GENERALIZATION OF A CYCLOTOMIC FORMULA*

BY H. S. GRANT

1. Introduction. Jacobi stated without proof† the following cyclotomic formula

\[ F(-1) \cdot F(\alpha^2) = \alpha^{2m} F(\alpha) \cdot F(-\alpha), \]

where

\[ F(\alpha) = x + \alpha x^q + \alpha^2 x^{q^2} + \cdots + \alpha^{q-2} x^{q^{q-2}}, \]

\( q \) is an odd prime, \( g \) a primitive root, mod \( q \), \( g^m \equiv 2 \), mod \( q \), \( x^q = 1 \) (\( x \neq 1 \)), \( \alpha^{q-1} = 1 \) (\( \alpha \neq 1 \)). This relation is essentially one involving Lagrange resolvent functions, and ultimately reduces to one connecting two Jacobi \( \psi \)-functions. The former have been generalized by L. Stickelberger,‡ and the latter by H. H. Mitchell.§

It is the purpose of this paper to generalize Jacobi's formula to the case \( q^t = 1 \), mod \( n \), \( q \) an odd prime, \( t \) any exponent for which the congruence holds, \( n \) even. If we take \( t = 1 \), \( n = q - 1 \), the relation stated above then follows as a special case. Before proceeding further, the reader is strongly advised to refer to Mitchell's paper mentioned above, frequent use of which is made in what follows.

2. Characteristic Properties of the Generalized Function. If

\[ s(x) = \sum_{i=0}^{t-1} a_i x^i, \]  

\( a_i \) reduced, mod \( q \), \( q \) prime, \( s(q) \) will represent a complete residue system, mod \( q^t \). We interpret \( s(x) \) as the marks of a Galois field of order \( q^t \). Let \( \epsilon \) denote a primitive \( n \)th root of unity, where \( q^t = 1 \), mod \( n \), and \( \tau \) a primitive \( q^t \)th root of unity. We define

\[ (\epsilon^\lambda, \tau) = \sum_s \epsilon^\lambda \text{ind} s(x) \tau^{s(q)}, \]

the summation being taken over all marks excepting 0, and the

---

* Presented to the Society, September 13, 1935.
index being taken with respect to a primitive root $g(x)$ in the Galois field. We set $q^t - 1 = kn$. For convenience of reference, we list the following characteristic properties of the function $(e^t, \tau)$.

1. $(1, \tau) = -1$.
2. $(e^t, \tau)(e^{-\lambda}, \tau) = (-1)^{\lambda}q^t, \quad q \text{ odd,}$
   
   $= q^t, \quad q = 2, \text{ provided } n \mid \lambda.$
3. $\frac{(e^t, \tau)(e^{-\mu}, \tau)}{(e^{t+\mu}, \tau)} = \Psi_{\lambda, \mu}(e)$, where

   $\Psi_{\lambda, \mu}(e) = \sum_s e^{s \text{ ind } \sigma_{-(\lambda+\mu) \text{ ind } (e+1),} (n \mid \lambda + \mu)},$

   $s$ goes over all the marks of our Galois field excepting 0 and $-1$ if $q$ is odd, and 0 and 1 if $q$ is 2.*

4. $\Psi_{\lambda, \mu}(e)\Psi_{\lambda, \mu}(e^{-1}) = q^t$,
   
   (a) $\Psi_{\lambda, \mu}(e)\Psi_{\lambda, \mu}(e) = \Psi_{\lambda, \mu}(e)$,

   where

   $\lambda, \mu, \lambda + \mu \neq 0 \text{ mod } n.$

5. Let $q_i = q(e^{i})$, where $ii' \equiv 1, \text{ mod } n,$ and $q_i$ is any prime ideal factor of $q$ in the cyclotomic number-realm $k(e)$. Further, let $i$ assume the $\phi(n)/t_i$ values prime to $n$ such that the quotient of no two of them is congruent, mod $n,$ to a power of $q,$ $t_i$ being the exponent to which $q$ belongs, mod $n.$ If $g^k \equiv e, \text{ mod } q^g(e),$ $g = g(e)$, then the principal ideal satisfies the relation

   $\left[\Psi_{\lambda, \mu}(e)\right] = \prod_i q_i^{m_i},$

   $m_i$ denoting the number of sums

   $| - \lambda iq^{t-i} | + | - \mu iq^{t-i} |, \quad (j = 0, 1, \ldots, t - 1),$

   whose values exceed $n$, $|x|$ being the least positive residue of $x$, mod $n$, and $\lambda, \mu, \lambda + \mu \neq 0, \text{ mod } n.$†

* Properties (1), (2), and (3) are analogous to those for the Lagrange function. Compare H. Weber, Lehrbuch der Algebra, 2nd ed., vol. 1, 1899, pp. 611–612.
† See H. H. Mitchell, loc. cit., for properties (4) and (5), particularly pages 168, 169, and 173.
Properties (1) and (2) show that \((\varepsilon^n, \tau) \neq 0\) for any \(\lambda\). Taking \(n\) as even, so that \(q\) must be an odd prime, we shall prove that

\[(A) \quad (\varepsilon^{n/2}, \tau)(\varepsilon^m, \tau) = \varepsilon^{2m\lambda}(\varepsilon^\lambda, \tau)(\varepsilon^{\lambda+n/2}, \tau),\]

where \(0 < \lambda < n\), \(\varepsilon^m \equiv 2\), mod \(q(\lambda)\), \(g = g(\lambda)\). As remarked in the introduction, this reduces to the Jacobi formula when \(n = q - 1\), \(g\) an odd prime, and \(t = 1\). We have replaced \(\alpha\) by \(\varepsilon^\lambda\), and \(x\) by \(\tau\).

3. The Cases \(\lambda \equiv \pm n/4\), mod \(n\). In either of the cases \(\lambda \equiv \pm n/4\), mod \(n\), (A) becomes by virtue of (2), and since \(\varepsilon^{n/2} = -1\),

\[
(-1)^{k \cdot n/2}q^t = (-1)^m(-1)^{k \cdot n/4}q^t,
\]

that is,

\[(B) \quad 1 = (-1)^m(-1)^{kn/4}.
\]

Since \(4 \mid n\), \(i\) is a number of \(k(\lambda)\). Now

\[g^{kn/2} + 1 = (g^{kn/4} - i)(g^{kn/4} + i) \equiv 0\), mod \(q(\lambda)\),
\]

whence \(\text{ind } i = \pm kn/4\). But \(2 = i(1 - i)^2\), therefore \(\text{ind } 2 = \text{ind } i + 2 \text{ ind } (1 - i), \text{mod } kn\), and consequently \(\text{ind } 2\) and \(\text{ind } i\) are both even or both odd, which establishes (B), since \(\text{ind } 2 = m\).

Excepting the above values of \(\lambda\), (A) becomes from property (3),

\[(C) \quad \Psi_{n/2, 2\lambda}(\varepsilon) = \varepsilon^{2m\lambda}\Psi_{\lambda, \lambda+n/2}(\varepsilon)\]

Equation (C) is evidently true for \(\lambda = n/2\), and it is only necessary to prove it for \(0 < \lambda < n/2\). For, if \(\lambda = n/2 + a\), \(0 < a < n/2\),

\[
\Psi_{n/2, 2\lambda}(\varepsilon) = \Psi_{n/2, 2a}(\varepsilon), \\
\Psi_{\lambda, \lambda+n/2}(\varepsilon) = \Psi_{n/2+a, a}(\varepsilon) = \Psi_{a, a+n/2}(\varepsilon).
\]

In what follows, we assume \(g^k \equiv \varepsilon\), mod \(q(\lambda)\), a restriction that we will remove later.

4. A Relation between the \(\Psi\)-Functions. Using (5), we have

\[\left[\Psi_{n/2, 2\lambda}(\varepsilon)\right] = \left[\Psi_{\lambda, \lambda+n/2}(\varepsilon)\right],\]

whence

\[\Psi_{n/2, 2\lambda}(\varepsilon) = E(\varepsilon)\Psi_{\lambda, \lambda+n/2}(\varepsilon),\]
where $E(e)$ is a unit. For, since $iq_{t-j}$ is odd,
\[
| (-n/2)iq_{t-j} | + | -2\lambda iq_{t-j} | = n/2 + 2 | -\lambda iq_{t-j} |
\]
\[
= | -\lambda iq_{t-j} | + | - (\lambda + n/2) iq_{t-j} |, \quad (j = 0, 1, \ldots, t - 1),
\]
when $| -\lambda iq_{t-j} | < n/2$, and,
\[
| (-n/2)iq_{t-j} | + | -2\lambda iq_{t-j} | = n/2 + 2 | -\lambda iq_{t-j} | - n
\]
\[
= | -\lambda iq_{t-j} | + | - (\lambda + n/2) iq_{t-j} |,
\]
when $| -\lambda iq_{t-j} | > n/2$. Replacing $e$ by $e^{-1}$, above, we have
\[
\Psi_{n/2,2\lambda}(e^{-1}) = E(e^{-1})\Psi_{\lambda,\lambda+n/2}(e^{-1}).
\]
Making use of (4a), we obtain $E(e)E(e^{-1}) = 1$, whence $E(e)$ is a root of unity, say $e^b$.* Now we have
\[
\Psi_{n/2,2\lambda}(e) = e^b\Psi_{\lambda,\lambda+n/2}(e).
\]
Since $g^k \equiv e$, mod $q(e)$, we have at once
\[
\Psi_{n/2,2\lambda}(g^k) \equiv g^{kb}\Psi_{\lambda,\lambda+n/2}(g^k), \quad \text{mod } q(e).
\]
Referring back to the definition of the $\Psi$-function in §2, we readily see that this congruence reduces to
\[
\sum_x g^{2k\lambda x}(g^x + 1)^{kv} \equiv g^{kb} \sum_x g^{k\lambda x}(g^x + 1)^{kv}, \quad \text{mod } q(e),
\]
where $2\lambda + n/2 + v \equiv 0$, mod $n$, and $x$ goes through all values $0, 1, \ldots, kn - 1$ excepting $kn/2$. Thus
\[
g^{kb} \equiv \frac{\sum_x g^{2k\lambda x}(g^x + 1)^{kv}}{\sum_x g^{k\lambda x}(g^x + 1)^{kv}}, \quad \text{mod } q(e),
\]
and we proceed to determine what the right-hand member of this congruence reduces to as a function of $g$, a primitive $(kn)$th root of unity.

5. The Determination of $b$. Since $g^{kn/2} = -1$, we may let $x$ take all values $0, 1, \ldots, kn - 1$. Now

\[
\sum_{x=0}^{kn-1} g^{2khx}(g^x + 1)^{kr} = \sum_{x=0}^{kn-1} g^{2khx} \sum_{h=0}^{kr} C_{kr,h} g^{(kr-h)x} \\
= \sum_{h=0}^{kr} C_{kr,h} \sum_{x=0}^{kn-1} g^{(2kh+kr-h)x},
\]

where \( C_{c,d} \) is the binomial coefficient \( c!d!(c-d)! \). But

\[
\sum_{x=0}^{kn-1} g^{tx} = \frac{(g^t)^{kn} - 1}{g^t - 1} = 0 \text{ or } kn,
\]

according as \( kn \) does not or does divide \( l \). Taking \( 0 < v < n \), we have, since \( 0 < \lambda < n/2 \), \( v = n/2 - 2\lambda \) or \( 3n/2 - 2\lambda \) according as \( \lambda < n/4 \) or \( \lambda > n/4 \). In the first case, \( 2kh + kv - h \leq kn/2 \), and, in the second, \( 2kh + kv - h = 3kn/2 - h = kn \), when \( h = kn/2 \). From these considerations, we have

\[
\sum_{x=0}^{kn-1} g^{2khx}(g^x + 1)^{kr} = (kn) C_{skn/2-2kh, kn/2},
\]

provided \( n/4 < \lambda < n/2 \).*

Similarly

\[
\sum_{x=0}^{kn-1} g^{khx}(g^x + 1)^{kr} = (kn) C_{3kn/2-2kh, kn/2-kh},
\]

under the same restrictions for \( \lambda \). We now have

\[
\frac{\sum_{x=0}^{kn-1} g^{2khx}(g^x + 1)^{kr}}{\sum_{x=0}^{kn-1} g^{khx}(g^x + 1)^{kr}} = \frac{(kn/2 - kh)!(kn - kh)!}{(kn/2)!(kn - 2kh)!},
\]

provided \( n/4 < \lambda < n/2 \). This last quotient is

\[
\frac{(kn - k\lambda)(kn - k\lambda - 1) \cdots (kn - 2k\lambda + 1)}{(kn/2)(kn/2 - 1) \cdots (kn/2 - k\lambda + 1)} \\
= \frac{2^{kh}(kn - k\lambda)(kn - k\lambda - 1) \cdots (kn - 2k\lambda + 1)}{(kn)(kn - 2) \cdots (kn - 2k\lambda + 2)} \\
= \frac{2^{kh}(q^t - 2k\lambda)(q^t - 2k\lambda + 1) \cdots (q^t - k\lambda - 1)}{(q^t - 1)(q^t - 3) \cdots (q^t - 2k\lambda + 1)}
\]

\[ q^i - (2k\lambda - i) = q^{s_i}(q^{t-s_i} - k_i), \]
\[ q^i - (2i + 1) = q^{s_i}(q^{t-s_i} - l_i), \]
so that both \( k_i \) and \( l_i \) are prime to \( q \), and \( s_i, t_i < t \), since \( 2k\lambda < q^t - 1 \). Then our quotient becomes
\[ 2^{k\lambda} \prod_{i=0}^{k\lambda-1} \frac{q^{s_i}(q^{t-s_i} - k_i)}{q^{s_i}(q^{t-s_i} - l_i)}. \]

But
\[ \prod_{i=0}^{k\lambda-1} \frac{q^{s_i}k_i}{q^{s_i}l_i} = \frac{(2k\lambda)(2k\lambda - 1) \cdots (k\lambda + 1)}{1 \cdot 3 \cdot 5 \cdots (2k\lambda - 1)} = \frac{(2k\lambda)!}{[1 \cdot 3 \cdot 5 \cdots (2k\lambda - 1)](k\lambda)!} = 2^{k\lambda}. \]

Therefore, since \( q \) is an odd prime, and \( k_i, l_i \) are prime to \( q \), we have \( \prod_{i=0}^{k\lambda-1} q^{s_i} = \prod_{i=0}^{k\lambda-1} q^{t-s_i} \). Our quotient is now
\[ 2^{k\lambda} \prod_{i=0}^{k\lambda-1} \frac{(q^{t-s_i} - k_i)}{(q^{t-s_i} - l_i)}, \]
which is congruent to \( 2^{k\lambda} \prod_{i=0}^{k\lambda-1} k_i/l_i = 2^{2k\lambda} \mod q(e) \). Since \( 2 \equiv g^m \mod q(e) \), it follows from the previous section that
\[ g^{kb} \equiv g^{2k\lambda e}, \mod q(e), \]
whence
\[ kb = 2km\lambda, \mod kn, \]
\[ b \equiv 2m\lambda, \mod n. \]

6. Removal of the Restrictions. Equation (C) has been established when \( n/4 < \lambda < n/2 \), and \( g^k \equiv e, \mod q(e) \). Replacing \( e \) by \( e^{-1} \) in (C), we have
\[ \Psi_{n/2,2\lambda}(e^{-1}) = e^{-2m\lambda} \Psi_{\lambda,\lambda+n/2}(e^{-1}), \quad (n/4 < \lambda < n/2), \]
or
\[ \Psi_{n/2, -2\lambda}(\epsilon) = \epsilon^{-2m\lambda} \Psi_{-\lambda, -\lambda + n/2}(\epsilon), \]

that is,

\[ \Psi_{n/2, 2\mu}(\epsilon) = \epsilon^{2m\mu} \Psi_{\mu, \mu + n/2}(\epsilon), \quad (-n/2 < \mu < -n/4). \]

If \( \mu = \nu - n/2 \), we have

\[ \Psi_{n/2, 2\nu}(\epsilon) = \epsilon^{2m\nu} \Psi_{\nu, \nu + n/2}(\epsilon), \quad (0 < \nu < n/4). \]

To remove the restriction on \( g \), we introduce a simple change of notation, writing ((3), §2)

\[ \Psi_{a, b}(\epsilon, g) = \sum_s \epsilon^{b \cdot \text{ind}_g s - (a + b) \cdot \text{ind}_g (s + 1)}. \]

Referring to (C), we wish to show

\[ (C') \quad \Psi_{n/2, 2\lambda}(\epsilon, G) = \epsilon^{2m\lambda} \Psi_{\lambda, \lambda + n/2}(\epsilon, G), \]

where \( 0 < \lambda < n \), \( G^M \equiv 2 \), mod \( q(\epsilon) \), \( G \) being any primitive root of our Galois field. Let \( G \equiv g^z \), mod \( q(\epsilon) \), so that \( \text{ind}_g s \equiv s \) ind \( _g s \), mod \( kn \). Then

\[ \Psi_{a, b}(\epsilon', g) = \Psi_{a, b}(\epsilon, G), \]

where \( \epsilon \epsilon' \equiv 1 \), mod \( kn \). Replacing \( \epsilon \) by \( \epsilon' \) in (C), we have

\[ \Psi_{n/2, 2\lambda}(\epsilon', G) = \epsilon^{2m\lambda} \Psi_{\lambda, \lambda + n/2}(\epsilon', G), \]

or

\[ \Psi_{n/2, 2\lambda}(\epsilon, G) = \epsilon^{2m\lambda} \Psi_{\lambda, \lambda + n/2}(\epsilon, G). \]

Writing \( M \) for \( mz' \), we have

\[ G^M = G^{mz'} \equiv g^{mz'} \equiv g^m \equiv 2, \text{ mod } q(\epsilon), \]

and (C') is established.

Rutgers University