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

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

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 ψ-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 $q^t \equiv 1$, 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 ϵ denote a primitive nth root of unity, where $q^t \equiv 1$, mod n, and τ a primitive q^tth 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.

† Journal für Mathematatik, vol. 30 (1846), p. 167.

‡ Mathematische Annalen, vol. 37 (1890), pp. 321–367.

§ Transactions of this Society, vol. 17 (1916), pp. 165–177.

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 (ϵ^λ, τ).

$$(1) \qquad (1, \tau) = -1.$$

$$(2) \qquad (\epsilon^\lambda, \tau)(\epsilon^{-\lambda}, \tau) = (-1)^{k\lambda} q^t, \qquad q \text{ odd},$$
$$= q^t,\ q = 2, \text{ provided } n \nmid \lambda.$$

$$(3) \qquad \frac{(\epsilon^\lambda, \tau)(\epsilon^{-\mu}, \tau)}{(\epsilon^{\lambda+\mu}, \tau)} = \Psi_{\lambda,\mu}(\epsilon),$$

where

$$\Psi_{\lambda,\mu}(\epsilon) = \sum_s \epsilon^{\mu \text{ ind } s - (\lambda+\mu) \text{ ind } (s+1)}, \qquad (n \nmid \lambda + \mu),$$

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.*

$$(4) \quad \begin{array}{ll} \text{(a)} & \Psi_{\lambda,\mu}(\epsilon)\Psi_{\lambda,\mu}(\epsilon^{-1}) = q^t, \\ \text{(b)} & \Psi_{\lambda,\mu}(\epsilon^q) = \Psi_{\lambda,\mu}(\epsilon), \end{array}$$

where

$$\lambda,\ \mu,\ \lambda + \mu \not\equiv 0 \mod n.$$

(5) Let $q_i = q(\epsilon^{i'})$, where $ii' \equiv 1$, mod n, and q_i is any prime ideal factor of q in the cyclotomic number-realm $k(\epsilon)$. Further, let i assume the $\phi(n)/t_1$ values prime to n such that the quotient of no two of them is congruent, mod n, to a power of q, t_1 being the exponent to which q belongs, mod n. If $g^k \equiv \epsilon$, mod $q(\epsilon)$, $g = g(\epsilon)$, then the principal ideal satisfies the relation

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

m_i denoting the number of sums

$$\left| -\lambda i q^{t-j} \right| + \left| -\mu i q^{t-j} \right|, \qquad (j = 0, 1, \cdots, t-1),$$

whose values exceed n, $|x|$ being the least positive residue of x, mod n, and λ, μ, $\lambda + \mu \not\equiv 0$, 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 $(\epsilon^\lambda, \tau)\neq 0$ for any λ. Taking n as even, so that q must be an odd prime, we shall prove that

$$(\epsilon^{n/2}, \tau)(\epsilon^{2\lambda}, \tau) = \epsilon^{2m\lambda}(\epsilon^\lambda, \tau)(\epsilon^{\lambda+n/2}, \tau), \tag{A}$$

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

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 $\epsilon^{n/2}=-1$,

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

that is,

$$1 = (-1)^m(-1)^{kn/4}. \tag{B}$$

Since $4\,|n$, i is a number of $k(\epsilon)$. Now

$$g^{kn/2}+1 = (g^{kn/4}-i)(g^{kn/4}+i)\equiv 0, \text{ mod } q(\epsilon),$$

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

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

$$\Psi_{n/2,2\lambda}(\epsilon) = \epsilon^{2m\lambda}\Psi_{\lambda,\lambda+n/2}(\epsilon). \tag{C}$$

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

$$\Psi_{n/2,2\lambda}(\epsilon) = \Psi_{n/2,2a}(\epsilon)$$
$$\Psi_{\lambda,\lambda+n/2}(\epsilon) = \Psi_{n/2+a,a}(\epsilon) = \Psi_{a,a+n/2}(\epsilon).$$

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

4. *A Relation between the* Ψ-*Functions*. Using (5), we have

$$[\Psi_{n/2,2\lambda}(\epsilon)] = [\Psi_{\lambda,\lambda+n/2}(\epsilon)],$$

whence

$$\Psi_{n/2,2\lambda}(\epsilon) = E(\epsilon)\Psi_{\lambda,\lambda+n/2}(\epsilon),$$

where $E(\epsilon)$ is a unit. For, since iq^{t-j} is odd,

$$\begin{aligned}|(-n/2)iq^{t-j}| + |-2\lambda iq^{t-j}| &= n/2 + 2|-\lambda iq^{t-j}| \\ &= |-\lambda iq^{t-j}| + |-(\lambda + n/2)iq^{t-j}|, \quad (j = 0, 1, \cdots, t-1),\end{aligned}$$

when $|-\lambda iq^{t-j}| < n/2$, and,

$$\begin{aligned}|(-n/2)iq^{t-j}| + |-2\lambda iq^{t-j}| &= n/2 + 2|-\lambda iq^{t-j}| - n \\ &= |-\lambda iq^{t-j}| + |-(\lambda + n/2)iq^{t-j}|,\end{aligned}$$

when $|-\lambda iq^{t-j}| > n/2$. Replacing ϵ by ϵ^{-1}, above, we have

$$\Psi_{n/2,2\lambda}(\epsilon^{-1}) = E(\epsilon^{-1})\Psi_{\lambda,\lambda+n/2}(\epsilon^{-1}).$$

Making use of (4a), we obtain $E(\epsilon)E(\epsilon^{-1}) = 1$, whence $E(\epsilon)$ is a root of unity, say ϵ^b.* Now we have

$$\Psi_{n/2,2\lambda}(\epsilon) = \epsilon^b\Psi_{\lambda,\lambda+n/2}(\epsilon).$$

Since $g^k \equiv \epsilon$, mod $q(\epsilon)$, we have at once

$$\Psi_{n/2,2\lambda}(g^k) \equiv g^{kb}\Psi_{\lambda,\lambda+n/2}(g^k), \text{ mod } q(\epsilon).$$

Referring back to the definition of the Ψ-function in §2, we readily see that this congruence reduces to

$$\sum_x g^{2k\lambda x}(g^x + 1)^{k\nu} \equiv g^{kb}\sum_x g^{k\lambda x}(g^x + 1)^{k\nu}, \text{ mod } q(\epsilon),$$

where $2\lambda + n/2 + \nu \equiv 0$, mod n, and x goes through all values $0, 1, \cdots, kn-1$ excepting $kn/2$. Thus

$$g^{kb} \equiv \frac{\sum_x g^{2k\lambda x}(g^x + 1)^{k\nu}}{\sum_x g^{k\lambda x}(g^x + 1)^{k\nu}}, \text{ mod } q(\epsilon),$$

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 $0, 1, \cdots, kn-1$. Now

---

* See D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, 1932, Theorem 48, §21; R. Fricke, *Lehrbuch der Algebra*, vol. 3, 1928, p. 200.

$$\sum_{x=0}^{kn-1} g^{2k\lambda x}(g^x+1)^{k\nu} = \sum_{x=0}^{kn-1} g^{2k\lambda x}\sum_{h=0}^{k\nu} C_{k\nu,h}g^{(k\nu-h)x}$$
$$= \sum_{h=0}^{k\nu} C_{k\nu,h}\sum_{x=0}^{kn-1} g^{(2k\lambda+k\nu-h)x},$$

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

$$\sum_{x=0}^{kn-1} g^{lx} = \frac{(g^l)^{kn}-1}{g^l-1} = 0 \text{ or } kn,$$

according as kn does not or does divide l. Taking $0<\nu<n$, we have, since $0<\lambda<n/2$, $\nu=n/2-2\lambda$ or $3n/2-2\lambda$ according as $\lambda<n/4$ or $\lambda>n/4$. In the first case, $2k\lambda+k\nu-h\leqq kn/2$, and, in the second, $2k\lambda+k\nu-h=3kn/2-h=kn$, when $h=kn/2$. From these considerations, we have

$$\sum_{x=0}^{kn-1} g^{2k\lambda x}(g^x+1)^{k\nu} = (kn)C_{3kn/2-2k\lambda,\, kn/2},$$

provided $n/4<\lambda<n/2$.*

Similarly

$$\sum_{x=0}^{kn-1} g^{k\lambda x}(g^x+1)^{k\nu} = (kn)C_{3kn/2-2k\lambda,\, kn/2-k\lambda},$$

under the same restrictions for λ. We now have

$$\frac{\sum_{x=0}^{kn-1} g^{2k\lambda x}(g^x+1)^{k\nu}}{\sum_{x=0}^{kn-1} g^{k\lambda x}(g^x+1)^{k\nu}} = \frac{(kn/2-k\lambda)!(kn-k\lambda)!}{(kn/2)!(kn-2k\lambda)!},$$

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

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

* Compare H. Weber, loc. cit., pp. 620–621.

$$= 2^{k\lambda} \prod_{i=0}^{k\lambda-1} \left[\frac{q^t - (2k\lambda - i)}{q^t - (2i + 1)} \right].$$

Now let

$$q^t - (2k\lambda - i) = q^{s_i}(q^{t-s_i} - k_i),$$
$$q^t - (2i + 1) = q^{t_i}(q^{t-t_i} - l_i),$$

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

$$2^{k\lambda} \prod_{i=0}^{k\lambda-1} \frac{q^{s_i}(q^{t-s_i} - k_i)}{q^{t_i}(q^{t-t_i} - l_i)}.$$

But

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

Therefore, since q is an odd prime, and k_i, l_i are prime to q, we have $\prod_{i=0}^{k\lambda-1} q^{s_i} = \prod_{i=0}^{k\lambda-1} q^{t_i}$. Our quotient is now

$$2^{k\lambda} \prod_{i=0}^{k\lambda-1} \frac{(q^{t-s_i} - k_i)}{(q^{t-t_i} - l_i)}$$

which is congruent to $2^{k\lambda} \prod_{i=0}^{k\lambda-1} k_i/l_i = 2^{2k\lambda}$, mod $q(\epsilon)$. Since $2 \equiv g^m$, mod $q(\epsilon)$, it follows from the previous section that

$$g^{kb} \equiv g^{2km\lambda}, \text{ mod } q(\epsilon),$$

whence

$$kb \equiv 2km\lambda, \text{ mod } kn,$$
$$b \equiv 2m\lambda, \text{ mod } n.$$

6. *Removal of the Restrictions.* Equation (C) has been established when $n/4 < \lambda < n/2$, and $g^k \equiv \epsilon$, mod $q(\epsilon)$. Replacing ϵ by ϵ^{-1} in (C), we have

$$\Psi_{n/2,2\lambda}(\epsilon^{-1}) = \epsilon^{-2m\lambda}\Psi_{\lambda,\lambda+n/2}(\epsilon^{-1}), \qquad (n/4 < \lambda < n/2),$$

or

$$\Psi_{n/2,-2\lambda}(\epsilon) = \epsilon^{-2m\lambda}\Psi_{-\lambda,-\lambda+n/2}(\epsilon),$$

that is,

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

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

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

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

$$\Psi_{a,b}(\epsilon, g) = \sum_s \epsilon^{b \operatorname{ind}_g s-(a+b) \operatorname{ind}_g (s+1)}.$$

Referring to (C), we wish to show

(C′) $$\Psi_{n/2,2\lambda}(\epsilon, G) = \epsilon^{2M\lambda}\Psi_{\lambda,\lambda+n/2}(\epsilon, G),$$

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 ind $_g s\equiv z$ ind $_G s$, mod kn. Then

$$\Psi_{a,b}(\epsilon^{z'}, g) = \Psi_{a,b}(\epsilon, G),$$

where $zz'\equiv 1$, mod kn. Replacing ϵ by $\epsilon^{z'}$ in (C), we have

$$\Psi_{n/2,2\lambda}(e^{z'}, g) = \epsilon^{2m\lambda z'}\Psi_{\lambda,\lambda+n/2}(\epsilon^{z'}, g),$$

or

$$\Psi_{n/2,2\lambda}(\epsilon, G) = \epsilon^{2m\lambda z'}\Psi_{\lambda,\lambda+n/2}(\epsilon, G).$$

Writing M for mz', we have

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

and (C′) is established.

RUTGERS UNIVERSITY