JOURNAL OF NUMBER THEORY 1, 280–290 (1969)

Mixed Cyclotomy, Prime-Power Circulants, and Cyclotomy Modulo $p = ef+1$ for Composite e

THOMAS STORER*

Department of Mathematics,
University of Michigan, Ann Arbor, Michigan 48104

Communicated by D. J. Lewis

Received August 30, 1968

An explicit formula for the cyclotomic numbers modulo prime $p \equiv 1 \pmod{ee'}$ is given in terms of the cyclotomic numbers for p, e and p, e', and the mixed cyclotomic numbers $p,(e', e)$ when g.c.d. $(e, e') = 1$. The derivation of this formula depends upon the invertibility of the circulant coefficient matrix of a system of linear equations involving the respective periods; the determinant of this matrix is shown to be, in fact, a power of p.

1. INTRODUCTION

Let $p = (ee')f''+1$ be a prime with e, e' natural numbers greater than 1 such that $(e, e') = 1$. In this paper we introduce the *mixed cyclotomic numbers* $(i, j)_{(e)}^{(e)}$, modulo p and exhibit a large class of circulant matrices based upon these constants whose determinants (up to sign) are powers of p. We then use these constants, together with the (ordinary) cyclotomic numbers for p, e and p, e', to derive an explicit formula for the cyclotomic numbers for p, ee'. Results in this direction for the special cases *e twice an odd prime* and *e four times an odd prime* have been previously discussed in [2] and [3], respectively, and the reader is referred to [2] for additional results. The notation and results covering the ordinary cyclotomic-numbers for p, e will be as in [1].

2. DEVELOPMENT OF THE THEORY

Let e, e' be relatively prime natural numbers greater than 1 and let $p \equiv 1 \pmod{ee'}$ be prime. Write

$$p = ef+1 = e'f'+1 = (ee')f''+1$$

and denote the cyclotomic numbers and the periods for p, e and a fixed primitive root g modulo p by $(i,j)^{(e)}$ and $\eta_k^{(e)}$, respectively. The similar

* Supported in part by a research grant of the National Science Foundation.

notation for the cyclotomies corresponding to p, e' and p, ee' will always mean *with respect to the* (*same*) *fixed generator* g. We now state a lemma which will enable us to express the periods for p, ee' in terms of those for p, e and p, e'.

LEMMA 1. *Define* $\lambda = \exp(2\pi i/p)$ *and let* $\bar{e}$ *be defined* modulo e' *by the congruence* $e\bar{e} \equiv 1 \pmod{e'}$. Then

$$p\eta^{(ee')}_{(1-e\bar{e})i+e\bar{e}j} = \sum_{s=0}^{f-1} \sum_{t=0}^{f'-1} \lambda^{g^{es+i}} \left\{1 + \sum_{h=1}^{p-1} \lambda^{g^h(g^{es+i}-g^{e't+j})}\right\}.$$

where $i = 0, 1, \ldots, e-1; j = 0, 1, \ldots, e'-1$.

Proof. The contribution of the inner bracket to the sum on the right is nonzero (i.e. is p) only if $g^{es+i} \equiv g^{e't+j} \pmod p$, in which case $es+i \equiv j \pmod{e'}$. Hence, with the above choice of $\bar{e}$, we find that $es+i \equiv (i-e\bar{e})i+e\bar{e}j \pmod{ee'}$, the right side of which is independent of s. ■

It is now convenient to introduce the *mixed cyclotomic numbers* $(i, j)^{(e)}_{(e')}$ for p and the (same) fixed generator g, defined to be the number of solutions to the congruence

$$z_i + 1 \equiv z_j \pmod p \qquad (z_i \in C^{(e')}_i,\ z_j \in C^{(e)}_j);$$

that is, the number of ordered pairs s, t with $0 \le s \le f'-1$; $0 \le t \le f-1$ such that

$$g^{e's+i} + 1 \equiv g^{et+j} \pmod p.$$

We now use Lemma 1 to express the $\eta^{(ee')}_k$ in terms of the mixed cyclotomic numbers $(i, j)^{(e)}_{(e')}$ and the $\eta^{(e)}_i \eta^{(e')}_j$ Note that, since $(e, e') = 1$, we may assume that e' is odd, so that $\eta^{(e')}_k = \overline{\eta^{(e')}_k}$ (conjugate) is real for all k.

LEMMA 2. *Assuming e' odd, we have*

$$p\eta^{(ee')}_{(i-e\bar{e})i+e\bar{e}j} = \sum_{h=0}^{e'-1} \sum_{k=0}^{e-1} [(h, k)^{(e)}_{(e')} - f\delta^{(e')}_{h,0} - f'\delta^{(e)}_{k,0}]\eta^{(e)}_{i+k}\eta^{(e')}_{j+h},$$

where $\delta^{(n)}_{i,j} = \begin{cases} 1 \textit{ if } i \equiv j \pmod n \\ 0 \textit{ otherwise.} \end{cases}$

Proof. From Lemma 1, we have

$$\begin{aligned} p\eta^{(ee')}_{(i-e\bar{e})i+e\bar{e}j} &= \sum_{s=0}^{f-1} \sum_{t=0}^{f'-1} \lambda^{g^{es+i}} \left\{1 + \sum_{h=1}^{p-1} \lambda^{g^h(g^{es+i}-g^{e't+j})}\right\} \\ &= f'\eta^{(e)}_i + \sum_{h=1}^{p-1} \left(\sum_{s=0}^{f-1} \lambda^{(g^h+1)g^{es+i}}\right)\overline{\left(\sum_{t=0}^{f'-1} \lambda^{g^h g^{e't+i}}\right)} \\ &= f'\eta^{(e)}_i + f\eta^{(e')}_j + \sum_{h=1}^{p-1} \eta^{(e)}_{i+\operatorname{ind}(h+1)}\eta^{(e')}_{j+\operatorname{ind}(h)} \\ &= f'\eta^{(e)}_i + f\eta^{(e')}_j + \sum_{h=0}^{e'-1} \sum_{k=0}^{e-1} (h, k)^{(e)}_{(e')}\eta^{(e)}_{i+k}\eta^{(e')}_{j+h}. \end{aligned}$$

which is the lemma. ■

An inverse relation to that given in Lemma 2 is given in the following lemma.

LEMMA 3.

$$\eta_i^{(e)}\eta_j^{(e')} = \sum_{k=0}^{ee'-1} [(j-k, i-k)_{(e')}^{(e)} - f'']\eta_k^{(ee')}$$

for $i = 0, 1, \ldots, e-1; j = 0, 1, \ldots, e'-1$.

Proof. We have

$$\eta_i^{(e)}\eta_j^{(e')} = \left(\sum_{m=0}^{f-1} \lambda^{g^{em+i}}\right)\left(\sum_{n=0}^{f'-1} \lambda^{g^{e'n+j}}\right)$$
$$= \sum_{m=0}^{f-1} \sum_{n=0}^{f'-1} \lambda^{g^{em+i}-g^{e'n+j}}.$$

Let $N = g^{em+i} - g^{e'n+j}$ so that, as m and n vary over their respective ranges, we have $N \equiv 0 \pmod p$ exactly $|C_i^{(e)} \cap C_j^{(e')}| = f''$ times. On the other hand, for fixed m and n such that $N \not\equiv 0 \pmod p$, there exist integers u and k such that $N \equiv g^{ee'u+k} \pmod p$, whence

$$g^{e'(n-eu)+(j-k)} + 1 \equiv g^{e(m-e'u)+(i-k)} \pmod p.$$

The lemma now follows from the fact that $(e'n-em)+(j-i)$ runs over a complete residue system modulo ee' whenever n and m run over complete systems modulo e and e', respectively. ■

The coefficient matrix of the ee' linear relations of Lemma 3 is the circulant matrix $\mathscr{C}$ whose first row is given by

$$[(j, i)_{(e')}^{(e)} - f'', (j-1, i-1)_{(e')}^{(e)} - f'', \ldots, (j+1, i+1)_{(e')}^{(e)} - f''].$$

and, in view of Lemma 2, one might hopefully expect the value of its determinant Δ to be $\pm p$. We shall show that, in fact, the correct value is $\Delta = (-1)^{ee'} p^{\frac{1}{2}(e-1)(e'-1)}$, but to do this we need to develop the elementary relationships between the mixed cyclotomic numbers.

First we remark that the mixed cyclotomic numbers are given in terms of the cyclotomic numbers for p, ee' by the formula

$$(h, k)_{(e')}^{(e)} = \sum_{s=0}^{e-1} \sum_{t=0}^{e'-1} (e's+h, et+k)^{(ee')},$$

and we use this as a check on Lemma 2 by verifying that the sum of the $\eta_k^{(ee')}$ is -1. Here

$$p \sum_{i=0}^{e-1} \sum_{j=0}^{e'-1} \eta_{(i-e\bar{e})i+e\bar{e}j}^{(ee')} = \sum_{i,k=0}^{e-1} \sum_{j,h=0}^{e'-1} [(h, k)_{(e')}^{(e)} - f\delta_{h,0}^{(e')} - f'\delta_{k,0}^{(e)}]\eta_{i+k}^{(e)}\eta_{j+h}^{(e')}$$
$$= -e'f' - ef + \sum_{k,s=0}^{e-1} \sum_{h,t=0}^{e'-1} (e's+h, et+k)^{(ee')}$$
$$= -2p + 2 + (ee'f'' - 1) = -p,$$

where we have used the fact that

$$\sum_{k=0}^{e-1} \eta_k^{(e)} = -1.$$

LEMMA 4. *If $e, e' > 1$ are integral, then*

$$\text{(a)} \qquad (h, k)^{(e)}_{(e')} = \begin{cases} (k, h)^{(e')}_{(e)} & \textit{if } f'' \textit{ is even} \\ \left(k + \dfrac{ee'}{2}, h + \dfrac{ee'}{2}\right)^{(e')}_{(e)} & \textit{if } f'' \textit{ is odd.} \end{cases}$$

$$\text{(b)} \qquad \sum_{k=0}^{e-1} (h, k)^{(e)}_{(e')} = f' - \theta_h^{(e')}; \quad h = 0, 1, \ldots, e'-1.$$

$$\text{(c)} \qquad \sum_{h=0}^{e'-1} (h, k)^{(e)}_{(e')} = f - \delta_{k,0}^{(e)}; \quad k = 0, 1, \ldots, e-1.$$

We remark that in part (b), since we are assuming e' odd,

$$\theta_h^{(e')} = \begin{cases} 1 \text{ if } f' \text{ even, } i = 0 \\ 1 \text{ if } f' \text{ odd, } \ i = e/2 \\ 0 \text{ otherwise} \end{cases}$$

may in this case be replaced by $\delta_{h,0}^{(e')}$, since then $-1 \in C_0^{(e')}$.

Proof.

$$\text{(a) } (h, k)^{(e)}_{(e')} = \sum_{s=0}^{e-1} \sum_{t=0}^{e'-1} (e's+h, et+k)^{(ee')}$$

$$= \begin{cases} \displaystyle\sum_{s=0}^{e-1} \sum_{t=0}^{e'-1} (et+k, e's+h)^{(ee')} & \text{if } f'' \text{ even} \\ \displaystyle\sum_{s=0}^{e-1} \sum_{t=0}^{e'-1} \left(et + k + \frac{ee'}{2}, e's + h + \frac{ee'}{2}\right)^{(ee')} & \text{if } f'' \text{ odd} \end{cases}$$

$$= \begin{cases} (k, h)^{(e')}_{(e)} & \text{if } f'' \text{ even} \\ \left(k + \dfrac{ee'}{2}, h + \dfrac{ee'}{2}\right)^{(e')}_{(e)} & \text{if } f'' \text{ odd.} \end{cases}$$

$$\text{(b)} \qquad \sum_{k=0}^{e-1} (h, k)^{(e)}_{(e')} = \sum_{k=0}^{e-1} (h, k)^{(e')} = f' - \theta_h^{(e')}$$

$$\text{(c)} \qquad \sum_{h=0}^{e'-1} (h, k)^{(e)}_{(e')} = \sum_{h=0}^{e'-1} (h, k)^{(e)} = f - \delta_{k,0}^{(e)}. \blacksquare$$

3. EVALUATION OF Δ

We are now prepared to give the evaluation of Δ.

THEOREM 1. $\Delta = (-1)^{ee} p^{(e-1)(e'-1)/2}$.

Proof. If $\mu_1 = 1, \mu_2, \mu_3, \ldots, \mu_{ee'}$ are the roots of $x^{ee'} = 1$, and if we define

$$\phi(\mu) = \sum_{k=0}^{ee'-1} [(j-k, i-k)^{(e)}_{(e')} - f'']\mu^k$$

then it is well-known (see [4], p. 445, for example) that Δ is given by

$$\Delta = \phi(\mu_1)\phi(\mu_2)\ldots\phi(\mu_{ee'}).$$

Now

$$\phi(\mu_1) = \sum_{k=0}^{ee'-1} [(j-k, i-k)^{(e)}_{(e')} - f''] = -1$$

by Lemma 4, and the remaining terms occur in complex conjugate pairs, with the exception of that term $\mu_i = -1$ when ee' is even. In this case we have

$$\phi(-1) = \sum_{k=0}^{ee'-1} (-1)^k[(j-k, i-k)^{(e)}_{(e')} - f''] = -1,$$

again by Lemma 4. Thus $\operatorname{Sgn}(\Delta) = (-1)^{ee'}$.

With the exceptions of $\phi(\pm 1)$, the f″ does not contribute to the sum $\phi(\mu)$, and hence, for the remaining terms we may fix $\mu = \exp(2\pi i/ee')$ and consider the terms

$$\phi(\mu^r) = \sum_{k=0}^{ee'-1} (j-k, i-k)^{(e)}_{(e')}\mu^{rk}$$

for $r \neq 0$, $ee'/2$.

It is now a considerable simplification to observe that, for these remaining terms $\phi(\mu^r)$, we have

$$\begin{aligned}
\phi(\mu^r) &= \sum_{k=0}^{ee'-1} (j-k, i-k)^{(e)}_{(e')}\mu^{rk} \\
&= \sum_{k=0}^{ee'-1} \sum_{s=0}^{e-1} \sum_{t=0}^{e'-1} (e's+j-k, et+i-k)^{(ee')}\mu^{rk} \\
&= \sum_{k=0}^{ee'-1} \mu^{rk} \sum_{s=0}^{e-1} \sum_{t=0}^{e'-1} (k, et-e's+i-j)^{(ee')}\mu^{r(e's+j)} \\
&= \mu^{r[(1-e'\bar{e}')j+e'\bar{e}'i]} \sum_{k=0}^{ee'-1} \mu^{rk} \sum_{h=0}^{ee'-1} \mu^{-e'\bar{e}'rh}(k, h)^{(ee')} \\
&= \mu^{r[(1-e'\bar{e}')j+e'\bar{e}'i]} \sum_{k=0}^{ee'-1} \sum_{s=0}^{e-1} \sum_{t=0}^{e'-1} (k, et-e's)^{(ee')}\mu^{r(e's+k)} \\
&= \mu^{r[(1-e'\bar{e}')j+e'\bar{e}'i]} \sum_{k=0}^{ee'-1} \sum_{s=0}^{e-1} \sum_{t=0}^{e'-1} (k, et-e's+k)^{(ee')}\mu^{-r(k-e's)} \\
&= \mu^{r[(1-e'\bar{e}')j+e'\bar{e}'i]} \sum_{k=0}^{ee'-1} (-k, -k)^{(e)}_{(e')}\mu^{rk},
\end{aligned}$$

where $\bar{e}'$ is defined modulo e by $e'\bar{e}' \equiv 1 \pmod{e}$. Since $\mu^r = -1$ is excluded in these terms, the product of the units of the $\phi(\mu^r)$ is 1 and hence we may, without loss, consider $\phi(\mu^r)$ to be given by

$$\phi(\mu^r) = \sum_{k=0}^{ee'-1} (-k, -k)^{(e)}_{(e')}\mu^{rk}.$$

The above observation has also shown that $\phi(\mu^r)$ may be replaced by

$$\phi(\mu^r) = \sum_{k=0}^{ee'-1} (-k,\ -k)^{(e)}_{(e')}\mu^{rk} = \sum_{k=0}^{ee'-1} \mu^{rk} \sum_{h=0}^{ee'-1} \mu^{-e'\bar{e}'rh}(k,\ h)^{(ee')},$$

which last sum is the Lagrange sum $R_{(ee')}(r(1-e'\bar{e}'), r)$ when ee' does not divide $r(1-e'\bar{e}')$ or $r(2-e'\bar{e}')$.

It is further convenient to notice that, given $m|e$ and $m'|e'$ $(m,\ m' > 1)$, the mixed cyclotomic numbers for m, m' are given in terms of those for e, e' by the formula

$$(i,\ j)^{(m)}_{(m')} = \sum_{s=0}^{m'-1} \sum_{t=0}^{m-1} \left(s\frac{e'}{m} + i,\ \ t\frac{e}{m} + j\right)^{(e)}_{(e')}.$$

Now, given $r < ee'$ with $(r, ee') = n > 1$ but neither $e|r$ nor $e'|r$, the corresponding term $\phi(\mu^{rk})$ in the expansion of Δ is

$$\sum_{k=0}^{ee'-1} (-k,\ -k)^{(e)}_{(e')}\mu^{rk} = \sum_{k=0}^{\frac{ee'}{n}-1} \sum_{s=0}^{n-1} \left(\frac{ee'}{n}s-k,\ \ \frac{ee'}{n}s-k\right)^{(e)}_{(e')} \gamma^{k\left(\frac{r}{n}\right)},$$

where $\gamma = \mu^n$. But since

$$\sum_{s=0}^{n-1} \left(\frac{ee'}{n}s-k,\ \ \frac{ee'}{n}s-k\right)^{(e)}_{(e')} = \sum_{s=0}^{m'-1} \sum_{t=0}^{m-1} \left(\frac{e'}{m'}s-k,\ \ \frac{e}{m}t-k\right)^{(e)}_{(e')},$$

the original sum reduces to

$$\sum_{k=0}^{\frac{ee'}{n}-1} \sum_{s=0}^{m'-1} \sum_{t=0}^{m-1} \left(\frac{e'}{m'}s-k,\ \ \frac{e}{m}t-k\right)^{(e)}_{(e')} \gamma^{k\left(\frac{r}{n}\right)} = \sum_{k=0}^{\frac{ee'}{n}-1} (-k,\ -k)^{(m)}_{(m')}\gamma^{k\left(\frac{r}{n}\right)}.$$

Now $\left(\frac{r}{n}, \frac{ee'}{n}\right) = 1$ so, replacing γ by the (primitive $\left(\frac{ee'}{n}\right)$th) root $\gamma_1 = \gamma^{r/n}$, we have

$$\sum_{k=0}^{ee'-1} (-k,\ -k)^{(e)}_{(e')}\mu^{rk} = \sum_{k=0}^{\frac{ee'}{n}-1} (-k,\ -k)^{(m)}_{(m')}\gamma_1^k,$$

which occurs in the expansion of the corresponding circulant of (the lower) order ee'/n.

If $(r, ee') = 1$, we say that the factor $\phi(\mu^r)$ in the expansion of Δ occurs *primitively;* otherwise *imprimitively*. If $(r, ee') > 1$ but neither $e|r$ nor $e'|r$, then we say that the imprimitive factor $\phi(\mu^r)$ is *properly* imprimitive. At this point we have shown that each properly imprimitive factor corresponding to a given e, e' arises primitively as a factor for some $m|e$ and $m'|e'$, whence (by the observation) it is a Lagrange sum and, therefore, a square root of p in $\mathbf{Z}(\mu)$. Clearly, the number of primitive and properly imprimitive factors $\phi(\mu^r)$ is $(e-1)(e'-1)$. It therefore remains to show that the value of each of the (nonproperly) imprimitive factors $\phi(\mu^r)$ is -1.

We now suppose that $\phi(\mu^r)$ is nonproperly imprimitive because $e|r$. Then we have

$$\begin{aligned}\sum_{k=0}^{ee'-1}(-k,-k)_{(e')}^{(e)}\mu^{rk} &= \sum_{k=0}^{ee'-1}\mu^{rk}\sum_{h=0}^{ee'-1}(k,h)^{(ee')}\\ &= -\sum_{k=0}^{ee'-1}\mu^{rk}\theta_k^{(ee')}\\ &= \begin{cases}-1 & \text{if } f'' \text{ is even}\\ -(-1)^r & \text{if } f'' \text{ is odd}\end{cases}\\ &= -1,\end{aligned}$$

since f'' odd implies ee' even, whence e (which divides r) is even by the hypothesis e' odd. Similarly, if $\phi(\mu^r)$ is nonproperly imprimitive because $e'|r$, we have

$$\sum_{k=0}^{ee'-1}(-k,-k)_{(e')}^{(e)}\mu^{rk} = \sum_{k=0}^{ee'-1}(a-k,a-k)_{(e)}^{(e')}\mu^{rk},$$

where

$$a = \begin{cases}0 & \text{if } f'' \text{ is even}\\ ee'/2 & \text{if } f'' \text{ is odd}\end{cases}$$

whence the sum in question becomes

$$\begin{aligned}\mu^{ra}\sum_{k=0}^{ee'-1}(-k,-k)_{(e)}^{(e')}\mu^{rk} &= \begin{cases}-\mu^{ra} & \text{if } f'' \text{ even}\\ -(-1)^{2ra} & \text{if } f'' \text{ odd}\end{cases}\\ &= -1\end{aligned}$$

by the analysis of the preceeding case, using the fact that $a=0$ if f'' is even.

This completes the proof of the theorem. ■

4. Determination of the Cyclotomic Constants

We now combine Lemmas 2 and 3 to obtain additional relations for the determination of the mixed cyclotomic numbers for p, e and e', and g.

THEOREM 2. *We have that*

$$p\eta_{(1-e\bar{e})i+e\bar{e}j}^{(ee')} = \sum_{s=0}^{ee'-1}\left\{\sum_{h=0}^{e'-1}\sum_{k=0}^{e-1}(h,k)_{(e')}^{(e)}(j+h-s,\, i+k-s)_{(e')}^{(e)} + \right.$$
$$\left. + f\delta_{s,j}^{(e')} + f'\delta_{s,i}^{(e)} - f''(p-2)\right\}\eta_s^{(ee')}.$$

Proof. Direct combination of Lemmas 2 and 3 yields

$$\begin{aligned} p\eta^{(ee')}_{(1-e\bar{e})i+e\bar{e}j} &= \sum_{h=0}^{e'-1}\sum_{k=0}^{e-1}\left[(h,k)^{(e)}_{(e')} - f\delta^{(e,)}_{h,0} - f'\delta^{(e)}_{k,0}\right]\times \\ &\qquad\times\sum_{s=0}^{ee'-1}\left[(j+h-s,\, i+k-s)^{(e)}_{(e')} - f''\right]\eta^{(ee')}_s \\ &= \sum_{s=0}^{ee'-1}\sum_{h=0}^{e'-1}\sum_{k=0}^{e-1}(h,k)^{(e)}_{(e')}(j+h-s,\, i+k-s)^{(e)}_{(e')}\eta^{(ee')}_s - \\ &\quad -f\sum_{s=0}^{ee'-1}(f'-\delta^{(e')}_{s,j})\eta^{(ee')}_s - \\ &\quad -f'\sum_{s=0}^{ee'-1}(f-\delta^{(e)}_{s,i})\eta^{(ee')}_s + eff'' - f'' - eff'' - e'f'f'', \end{aligned}$$

which is equivalent to the theorem. ■

COROLLARY.

$$\begin{aligned} \sum_{h=0}^{e'-1}\sum_{k=0}^{e-1}(h,k)^{(e)}_{(e')}(j+h-s,\, i+k-s)^{(e)}_{(e')} &= f''(p-2) + \\ &\quad + p\delta^{(ee')}_{s,(1-e\bar{e})i+e\bar{e}j} - f\delta^{(e')}_{s,j} - f\delta^{(e)}_{s,i}, \end{aligned}$$

for all $s = 0, 1, \ldots, ee'-1$; *in particular,*

$$\sum_{h=0}^{e'-1}\sum_{k=0}^{e-1}(h,k)^{(e)}_{(e')}(h-s,\, k-s)^{(e)}_{(e')} = f''(p-2) + p\delta^{(ee')}_{s,0} - f\delta^{(e')}_{s,0} - f'\delta^{(e)}_{s,0}.$$

Proof. The period equation is irreducible…

It is, of course, clear that the ee' equations in the above corollary are not independent. We show by example in the next section how Lemma 4 and this corollary can be combined to yield the mixed cyclotomic numbers for primes $p \equiv 1 \pmod 6$ with $e = 2$, $e' = 3$. First we give a formula for the cyclotomic numbers for p, ee' in terms of the cyclotomic numbers for p, e; p, e', and the mixed cyclotomic numbers.

THEOREM 3.

$$\begin{aligned} p^2((1-e\bar{e})i+e\bar{e}j,\, x)^{(ee')} &= f''p^2\theta^{(ee')}_{(1-e\bar{e})i+e\bar{e}j} + \\ &+ \sum_{m,h,s=0}^{e'-1}\ \sum_{n,k,t=0}^{e-1}\left[(m,n)^{(e)}_{(e')} - f\delta^{(e')}_{m,0} - f'\delta^{(e)}_{n,0}\right]\times \\ &\times\left[(h+m,\, k+n)^{(e)}_{(e')} - f\delta^{(e')}_{h+m,0} - f'\delta^{(e)}_{k+n,0}\right]\left[(i+k,\, t)^{(e)} - f\delta^{(e)}_{k,I-i}\right]\times \\ &\qquad\times\left[(j+h,\, s)^{(e')} - f'\delta^{(e')}_{h,-j}\right]\left[(m+s-x,\, n+t-x)^{(e)}_{(e')} - f''\right] \end{aligned}$$

where $-1 \in C^{(e)}_I$.

Proof. From Lemma 2, we have

$$\begin{aligned}
p^2\eta_0^{(ee')}\eta_{(1-e\bar{e})i+e\bar{e}j}^{(ee')} &= p^2\left\{\sum_{x=0}^{ee'-1}((1-e\bar{e})i+e\bar{e}j,\, x)^{(ee')}\eta_x^{(ee')}+f''\theta_{(1-e\bar{e})i+e\bar{e}j}^{(ee')}\right\}\\
&= \sum_{m,h=0}^{e'-1}\ \sum_{n,k=0}^{e-1}\left[(m,\, n)_{(e')}^{(e)}-f\delta_{m,0}^{(e')}-f'\delta_{n,0}^{(e)}\right]\times\\
&\qquad\times\left[(h,\, k)_{(e')}^{(e)}-f\delta_{h,0}^{(e')}-f'\delta_{k,0}^{(e)}\right]\eta_n^{(e)}\eta_{i+k}^{(e)}\eta_m^{(e')}\eta_{j+h}^{(e')}\\
&= \sum_{m,h,s=0}^{e'-1}\ \sum_{n,k,t=0}^{e-1}\left[(m,\, n)_{(e')}^{(e)}-f\delta_{m,0}^{(e')}-f'\delta_{n,0}^{(e)}\right]\times\\
&\qquad\times\left[(h+m,\, k+n)_{(e')}^{(e)}-f\delta_{h+m,0}^{(e')}-f'\delta_{k+n,0}^{(e)}\right]\times\\
&\qquad\times\left[(i+k,\, t)^{(e)}-f\delta_{k,I-i}^{(e)}\right]\times\\
&\qquad\times\left[(j+h,\, s)^{(e')}-f'\delta_{h,-j}^{(e')}\right]\eta_{n+t}^{(e)}\eta_{m+s}^{(e')}
\end{aligned}$$

which, after Lemma 3, is the theorem. ■

We remark that the right side of the expression in Theorem 3 above can be expanded and simplified, although with little apparent gain in insight. For example, using the Corollary to Theorem 2 and observing that

$$\theta_{(1-e\bar{e})i+e\bar{e}j}^{(ee')} = \delta_{(1-e\bar{e})i+e\bar{e}j,\,(1-e\bar{e})I}.$$

we may write

$$\begin{aligned}
p^2((1-e\bar{e})i+e\bar{e}j,\, x)^{(ee')} &= (f'')^2p^2-f''p^2(p-1)\theta_{(1-e\bar{e})i+e\bar{e}j}^{(ee')}\\
&\quad+\sum_{m,h,s=0}^{e'-1}\ \sum_{n,k,t=0}^{e-1}\left[(m,\, n)_{(e')}^{(e)}-f\delta_{m,0}^{(e')}-f'\delta_{n,0}^{(e)}\right]\times\\
&\quad\times\left[(h+m,\, k+n)_{(e')}^{(e)}-f\delta_{h+m,0}^{(e')}-f'\delta_{k+n,0}^{(e)}\right]\times\\
&\quad\times\left[(i+k,\, t)^{(e)}-f\delta_{k,I-i}^{(e)}\right]\left[(j+h,\, s)^{(e')}-f'\delta_{h,-j}^{(e')}\right]\times\\
&\quad\times(m+s-x,\, n+t-x)_{(e')}^{(e)},
\end{aligned}$$

and so forth.

5. Application to the Case $p \equiv 1 \pmod 6$

Let $p \equiv 1 \pmod 6$ be prime, and $e = 2$, $e' = 3$. Then the form of the mixed cyclotomic numbers from Lemma 4 is given by the matrix

A	B
C	D
E	F

and the elementary linear relations

$$\begin{aligned} A+B &= f'-1 \\ C+D &= f' \\ E+F &= f' \\ A+C+E &= f-1 \\ B+D+F &= f, \end{aligned}$$

only four of which are independent. Solving in terms of D and F, we have

$$\begin{aligned} A &= f'-f-1+D+F \\ B &= f-D-F \\ C &= f'-D \\ D &= D \\ E &= f'-F \\ F &= F. \end{aligned}$$

From the Corollary to Theorem 2, with $i=j=s=0$, we obtain the additional relation

$$A^2+B^2+C^2+D^2+E^2+F^2 = f''(p-2)+p-f-f',$$

whence, substitution yields

$$2D^2+2DF+2F^2-pD-pF+f''p = 0.$$

Multiplying this last equation by 18 we find, after combination and simplification, that

$$\begin{aligned} 6D &= p-x-3y \\ 6F &= p-x+3y, \end{aligned}$$

where $p = x^2+3y^2$ with $x \equiv 1 \pmod 3$, the sign of y being ambiguously determined. Hence we have

LEMMA 5. *The mixed cyclotomic numbers for $e = 2$, $e' = 3$, are given by the above array and the relations*

$$\begin{aligned} 6A &= p-5-2x \\ 6B &= p-3+2x \\ 6C &= p-2+x+3y \\ 6D &= p-x-3y \\ 6E &= p-2+x-3y \\ 6F &= p-x+3y \end{aligned}$$

where $p = x^2+3y^2$ and $x \equiv 1 \pmod 3$.

References

1. Storer, T. Cyclotomy and Difference Sets. *In* "Lectures in Advanced Mathematics," Vol. II. Markham (1967).

2. Dickson, L. E. Cyclotomy and trinomial congruences. *Trans. Am. Math. Soc.* **37** (1935), 363–380.

3. Whiteman, A. L. The cyclotomic numbers of order twelve. *Acta Arithmetica* **6** (1960), 53–76.

4. Muir, T. "A Treatise on the Theory of Determinants". Longmans, Green and Co., New York, 1933.