JOURNAL OF MATHEMATICAL ANALYSIS AND APPLICATIONS 25, 18–40 (1969)

The Number of Solutions of Some Equations in Galois Domains whose Orders are the Product of Three Distinct Odd Prime Powers

THOMAS STORER*

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

Submitted by C. L. Dolph

1. INTRODUCTION

If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where the p_i are distinct primes, and if we choose the ordered factorization $\phi_m = f_1 f_2 \cdots f_r$ of $\phi(m)$ into its characteristic factors, then it is well known that to each f_i there corresponds a residue class g_i of order f_i modulo m, such that every residue class a_j in the subgroup $\mathscr{M}_m$ of units modulo m may be expressed as

$$a_j \equiv g_1^{s_{1j}} g_2^{s_{2j}} \cdots g_r^{s_{rj}} \pmod{m} \qquad (0 \leqslant s_{ij} \leqslant f_i)$$

in exactly one way (see, for example, [1], p. 94). For fixed $\underline{g} = (g_1, g_2, \dots g_r)$ and $\underline{s} = (s_1, s_2, \dots s_r)$ we write

$$\underline{g}^{\underline{s}} \equiv g_1^{s_1} g_2^{s_2} \cdots g_r^{s_r} \pmod{m},$$

so that $\mathscr{M}_m = \{\underline{g}^{\underline{s}} : 0 \leqslant s_i < f_i\}$ and $\underline{g}^{\underline{s}} = \underline{g}^{\underline{t}}$ if and only if $\underline{s} = \underline{t}$. In this notation an important class of problems in number theory may be conveniently discussed at one time: namely, *for how many pairs* s_1, t_1, *with* $0 \leqslant s_1, t_1 < f_1$, *is the congruence*

$$\underline{g}^{\underline{s}} + 1 \equiv \underline{g}^{\underline{t}} \qquad \pmod{m}$$

satisfied. In the special cases $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 1$ and $k = 1$, $k = 2$, or $k = 3$, it has become customary (see [2]) to denote this number by $(s_1, t_1)_m$, the *cyclotomic number* corresponding to m, g_1, and the pair $(s_2, s_3, \dots, s_r)$, $(t_2, t_3, \dots, t_r)$; it is here proposed that the same designation prevail in the general case.

It is, perhaps, a curious fact that, given m and g_1, it is not the problem of establishing the existence of the g_i $(2 \leqslant i \leqslant r)$ which makes the determination of the numbers $(s_1, t_1)_m$ difficult; it is, rather, that the g_i are "too

* Partially supported by a NSF Research Grant.

numerous." That is, to each f_i there in general correspond several admissible g_i, and if g_i' be substituted for g_i, the distribution of the residues $a_j \in \mathscr{M}_m$ will apparently change (i.e., a_j will be represented by different $\underset{\sim}{s}$). It is therefore, prerequisite to the solution of our problem that a "canonical" representation of the residues of $\mathscr{M}_m$ in the above m be found. Hence we begin with a brief resumé of the known results for $m = p^\alpha$ and $m = p^\alpha q^\beta$.

2. Resumé 1: The Fields $GF(p^\alpha)$

We begin with the case $m = p = ef + 1$ an odd prime, so that the structure under consideration is the field $\mathbf{Z}_p$; here $\mathscr{M}_p$ is cyclic with *generator*, say, g. If we define the *cyclotomic classes*

$$C_{p,i} = \{g^{es+i} \pmod p) : s = 0, 1, \ldots, f-1\}$$

for $i = 0, 1, \ldots, e-1$, our problem is to determine the numbers $(i,j)_p$, $0 \leqslant i, j \leqslant e-1$, the number of solutions of the congruence

$$z_i + 1 \equiv z_j \pmod p) \qquad z_i \in C_{p,i}, \qquad z_j \in C_{p,j};$$

i.e., the number of ordered pairs (s, t) with $0 \leqslant s,\ t \leqslant f-1$ such that

$$g^{es+i} + 1 \equiv g^{et+j} \pmod p).$$

The matrix $\mathbf{C}_{p,e}$ whose ijth entry is the *cyclotomic number* $(i,j)_p$ is called the *cyclotomic matrix* of $\mathbf{Z}_p$ with respect to e and the fixed generator g. We remark that, since $\mathbf{Z}_p$ is unique up to isomorphism, replacement of g by a new generator g^* of $\mathscr{M}_p$ leaves $C_{p,0}$ fixed, and at most permutes the remaining $C_{p,i}$, $i \neq 0$.

The following relations between the cyclotomic numbers for $\mathbf{Z}_p$, e, and g are well known (see [2], p. 25):

Lemma 1.

(1) $(i,j)_p = (i+ne, j+me)_p \qquad$ *for all* $\qquad m, n \in \mathbf{Z}.$

(2) $(i,j)_p = (e-i, j-i)_p$,

(3) $$(i,j)_p = \begin{cases} (j,i)_p & \text{if} \quad f \text{ is even} \\ \left(j + \dfrac{e}{2}, i + \dfrac{e}{2}\right)_p & \text{if} \quad f \text{ is odd,} \end{cases}$$

(4) $\displaystyle\sum_{j=0}^{e-1} (i,j)_p = f - \theta_{p,i}$,

where

$$\theta_{p,i} = \begin{cases} 1 & \textit{if} \quad f \textit{ is even and} \quad i = 0 \\ 1 & \textit{if} \quad f \textit{ is odd and} \quad i = \frac{e}{2} \\ 0 & \textit{otherwise.} \end{cases}$$

We now introduce two arithmetic functions on $\mathbf{Z}_p$. To that end let N be a natural number and define

$$\lambda_N = \exp\left(\frac{2\pi i}{N}\right);$$

we then define the *periods* of $\mathbf{Z}_p$, g and e to be

$$\eta_{p,k} = \sum_{a \in C_{p,k}} \lambda_p{}^a = \sum_{s=0}^{f-1} \lambda_p^{g^{es+k}}$$

for $k = 0, 1, \ldots, e - 1$, and note that

$$\sum_{k=0}^{e-1} \eta_{p,k} = -1.$$

The periods are related to the cyclotomic numbers by the following lemma (see [2], p. 38).

LEMMA 2.

$$\eta_{p,0}\eta_{p,k} = \sum_{j=0}^{e-1} (k,j)_p\, \eta_{p,j} + f\theta_{p,k} \qquad \textit{for} \qquad k = 0, 1, \ldots, e - 1.$$

When e divides none of m, n, or $m + n$, we define the functions

$$F_p(\lambda_e^m) = \sum_{k=0}^{p-2} \lambda_e^{mk} \lambda_p^{g^k} = \sum_{k=0}^{e-1} \lambda_e^{mk} \eta_{p,k}$$

$$R_p(m, n) = \sum_{k=0}^{e-1} \lambda_e^{nk} \sum_{h=0}^{e-1} \lambda_e^{-(m+n)h} (k, h)_p .$$

The following properties of these functions are well known (see [2], pp. 41-47 and 62-64).

LEMMA 3.

(1) $\quad R_p(m, n) = \dfrac{F_p(\lambda_e^m)\, F_p(\lambda_e^n)}{F_p(\lambda_e^{m+n})}$.

(2) *If ℓ is the natural number determined by $g^{\ell} \equiv 2 \pmod{p}$, then*

$$F_p(-1)F_p(\lambda_e^{2k}) = \lambda_e^{2k\ell}F_p(\lambda_e^{k})F_p(-\lambda_e^{k}).$$

Part (2) of Lemma 3 is known as *Jacobi's Lemma*, and we remark that it, as well as all results listed in the present section remain true (see [2], Part I) if $\mathbf{Z}_p$ is replaced by $GF(p^{\alpha})$, each congruence, of course, then being replaced by equality (between elements of the field). Further, the method of generalizing from $\mathbf{Z}_p$ to $\mathbf{Z}_{p^{\alpha}}$ is given in [3], and hence we shall in the future, without loss, restrict ourselves to the case where m is square-free (corresponding to $\mathbf{Z}_m$).

3. Resumé 2: The Galois Domains $GD(p^{\alpha}q^{\beta})$

Now let $p = ef + 1$ and $q = ef' + 1$ be distinct odd primes with g.c.d. $(f, f') = 1$ (i.e., $e =$ g.c.d. $(p-1, q-1)$; the analysis for $p = ef + 1$ and $q = e'f' + 1$, where $e \neq e'$, follows the lines of development below, and is completely worked out in [4]). Let $d =$ l.c.m.$(p-1, q-1) = eff'$, and suppose that g is a fixed common primitive root of p and q. If $x \in \mathbf{Z}_{pq}$ be defined by

$$x \equiv g \pmod{p} \qquad \text{and} \qquad x \equiv 1 \pmod{q},$$

we define, as in the case for the finite field, the *cyclotomic classes* for[1] $\mathbf{Z}_{pq}$ and g to be

$$C_{pq,i} = \{g^s x^i \pmod{pq} : s = 0, 1, \dots, d-1\}$$

for $i = 0, 1, \dots, e-1$, and immediately verify that the $C_{pq,i}$ are pairwise disjoint and that their union is $\mathscr{M}_{pq}$. As before, the *cyclotomic numbers* $(i,j)_{pq}$, $0 \leqslant i, j \leqslant e-1$, for $\mathbf{Z}_{pq}$ and g are defined to be the number of solutions of the congruence

$$z_i + 1 \equiv z_j \pmod{pq} \qquad z_i \in C_{pq,i}, \qquad z_j \in C_{pq,j};$$

i.e., the number of ordered pairs (s, t) with $0 \leqslant s,\ t \leqslant d-1$ such that

$$g^s x^i + 1 \equiv g^t x^j \pmod{pq}.$$

The matrix $\mathbf{C}_{pq,e}$ whose ijth entry is the cyclotomic number $(i,j)_{pq}$ is called the *cyclotomic matrix* of $\mathbf{Z}_{pq}$ with respect to the fixed generator g. Now, however, replacement of the *generator* g by a new generator g^* may no longer leave $C_{pq,0}$ (nor, hence any $C_{pq,i}$) fixed, and so, in general, there exist

[1] We suppress the "e" now, as it is determined by p and q.

several distinct cyclotomic matrices $\mathbf{C}_{pq,e}$ for $\mathbf{Z}_{pq}$ which cannot be obtained one from another by permutations. Since $\phi(p-1)\,\phi(q-1)=\phi(e)\,\phi(d)$, it is easily shown, however, that there are at most $\phi(e)$ such matrices.*

While much work has been expended in the determination of the entries of $\mathbf{C}_{pq,e}$ (i.e., the cyclotomic numbers) through a detailed analysis of the structure of the domain $\mathbf{Z}_{pq}$, it might rather naturally be hoped that all the results derived for the fields $\mathbf{Z}_p$ and $\mathbf{Z}_q$ for e and the fixed generator g could be directly applied to give the corresponding information for $\mathbf{Z}_{pq}$. The first results in this direction were obtained in [5] through the introduction of characters on $\mathbf{Z}_{pq}$; the method below avoids this complication.

The following theorem is proved in [6].

THEOREM 1. *Let g be a common primitive root of the distinct odd primes $p=ef+1$ and $q=ef'+1$, where $e=$ g.c.d. $(p-1,q-1)$, and let P and Q be the permutation matrices*

$$P=\left(\begin{array}{c|c} 0 & I_{e-1} \\ \hline 1 & 0 \end{array}\right), \qquad Q=\left(\begin{array}{c|c} 0 & 1 \\ \hline I_{e-1} & 0 \end{array}\right).$$

Then

$$\mathbf{C}_{pq,e}=\mathbf{C}_{p,e}*\mathbf{C}_{q,e},$$

*where the matrix product $*$ is defined as follows: The ij*th *entry of $\mathbf{C}_p * \mathbf{C}_q$ is $(P^i\mathbf{C}_{p,e}Q^j)\cdot\mathbf{C}_{q,e}$, where "dot" denotes the inner product of the two matrices.*

Let us give a direct verification of this theorem for the simplest case, $e=2$. We assume, for the moment, that the cyclotomic matrices $\mathbf{C}_{pq,2}$ are known (see [2], pp. 92, 94 for the classical derivation based on the structure of the domain); here the result is an easy consequence of Lemma 4. In the case of the finite field, Lemma 1 is sufficient to determine the cyclotomic matrices $\mathbf{C}_{p,2}$ and, using this lemma, we find that

$$\mathbf{C}_{p,2}=\begin{cases}\begin{array}{|c|c|}\hline \dfrac{p-5}{4} & \dfrac{p-1}{4} \\ \hline \dfrac{p-1}{4} & \dfrac{p-1}{4} \\ \hline\end{array} & \text{if} \quad f \text{ is even} \\[2em] \begin{array}{|c|c|}\hline \dfrac{p-3}{4} & \dfrac{p+1}{4} \\ \hline \dfrac{p-3}{4} & \dfrac{p-3}{4} \\ \hline\end{array} & \text{if} \quad f \text{ is odd.}\end{cases}$$

* Here ϕ is the Euler function.

Now, $P = Q = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, whence Theorem 1 for $e = 2$ becomes

$$\mathbf{C}_{pq,2} = [(P^i \mathbf{C}_{p,2} P^j) \cdot \mathbf{C}_{q,2}],$$

which we directly verify.

CASE I: *ff' odd.* Then both f and f' are odd, so

$$\begin{aligned}(0,0)_{pq} &= \tfrac{1}{16}[3(p-3)(q-3)+(p+1)(q+1)] = \tfrac{1}{4}[(p-2)(q-2)+3],\\ (0,1)_{pq} &= \tfrac{1}{16}[(p+1)(q-3)+(p-3)(q+1)+2(p-3)(q-3)]\\ &= \tfrac{1}{4}[(p-2)(q-2)-1] = (1,0)_{pq} = (1,1)_{pq}.\end{aligned}$$

CASE II: *ff' even.* Then, since g.c.d. $(f, f') = 1$, either f is even and f' odd, or f' is even and f odd.

(a) *f even, f' odd.*

$$\begin{aligned}(0,0)_{pq} &= \tfrac{1}{16}[(p-5)(q-3)+(p-1)(q+1)+2(p-1)(q-3)]\\ &= \tfrac{1}{4}[(p-2)(q-2)+1] = (1,0)_{pq} = (1,1)_{pq},\\ (0,1)_{pq} &= \tfrac{1}{16}[(p-1)(q-3)+(p-5)(q+1)+2(p-1)(q-3)]\\ &= \tfrac{1}{4}[(p-2)(q-2)-3].\end{aligned}$$

(b) *f odd, f' even.*

$$\begin{aligned}(0,0)_{pq} &= \tfrac{1}{16}[(p-3)(q-5)+(p+1)(q-1)+2(p-3)(q-1)]\\ &= \tfrac{1}{4}[(p-2)(q-2)+1] = (1,0)_{pq} = (1,1)_{pq},\\ (0,1)_{pq} &= \tfrac{1}{16}[(p+1)(q-5)+3(p-3)(q-1)]\\ &= \tfrac{1}{4}[(p-2)(q-2)-3].\end{aligned}$$

Hence

$$\mathbf{C}_{pq,2} = \begin{cases} \begin{array}{|c|c|}\hline \dfrac{(p-2)(q-2)+1}{4} & \dfrac{(p-2)(q-2)-3}{4} \\ \hline \dfrac{(p-2)(q-2)+1}{4} & \dfrac{(p-2)(q-2)+1}{4} \\ \hline \end{array} & \text{if} \quad ff' \text{ is even} \\[4ex] \begin{array}{|c|c|}\hline \dfrac{(p-2)(q-2)+3}{4} & \dfrac{(p-2)(q-2)-1}{4} \\ \hline \dfrac{(p-2)(q-2)-1}{4} & \dfrac{(p-2)(q-2)-1}{4} \\ \hline \end{array} & \text{if} \quad ff' \text{ is odd,} \end{cases}$$

which is known to be the case. We remark that Theorem 1 can be directly proved as above for those e for which the cyclotomic matrices for $\mathbf{Z}_p$, $\mathbf{Z}_q$, and $\mathbf{Z}_{pq}$ are known. At present, this knowledge is limited by what is known for $\mathbf{Z}_{pq}$; namely, $e = 2$, 4, 6, and 8.

We also note that Theorem 1 provides us with an effective computational tool for determining the number of solutions to the types of equation which we have been considering, for the structures $GD(p^\alpha q^\beta)$ or $\mathbf{Z}_{p^\alpha q^\beta}$. In the examples below, the numbers of solutions for the summand fields were easily determined manually, the number for the domains from Theorem 1. Even for these relatively "small" examples, the amount of time saved through the use of Theorem 1 is considerable.

EXAMPLES.

Ia $pq = 65$; $e = 4$; $g = 2$, $x = 27$.

$$p = 5 = 4 \cdot 1 + 1, \qquad q = 13 = 4 \cdot 3 + 1,$$

$$\mathbf{C}_{5,4}: \begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&0&1\\\hline 0&0&0&0\\\hline 0&0&1&0\\\hline\end{array} \qquad \mathbf{C}_{13,4}: \begin{array}{|c|c|c|c|}\hline 0&1&2&0\\\hline 1&1&0&1\\\hline 0&1&0&1\\\hline 1&0&1&1\\\hline\end{array} \qquad \mathbf{C}_{65,4}: \begin{array}{|c|c|c|c|}\hline 3&0&2&4\\\hline 0&4&2&2\\\hline 2&2&2&2\\\hline 4&2&2&0\\\hline\end{array}\ g = 2$$

b: $g = 7$, $x = 27$.

$$\mathbf{C}_{5,4}: \begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&0&1\\\hline 0&0&0&0\\\hline 0&0&1&0\\\hline\end{array} \qquad \mathbf{C}_{13,4}: \begin{array}{|c|c|c|c|}\hline 0&0&2&1\\\hline 1&1&1&0\\\hline 0&1&0&1\\\hline 1&1&0&1\\\hline\end{array} \qquad \mathbf{C}_{65,4}: \begin{array}{|c|c|c|c|}\hline 0&2&3&4\\\hline 2&4&1&1\\\hline 3&1&3&1\\\hline 4&1&1&2\\\hline\end{array}\ g = 7$$

IIa : $pq = 85$; $e = 4$; $g = 3$, $x = 18$.

$$p = 5 = 4 \cdot 1 + 1\,, \qquad q = 17 = 4 \cdot 4 + 1\,,$$

$$\mathbf{C}_{5,4}: \begin{array}{|c|c|c|c|}\hline 0&0&0&1\\\hline 0&0&1&0\\\hline 0&0&0&0\\\hline 0&1&0&0\\\hline\end{array} \qquad \mathbf{C}_{17,4}: \begin{array}{|c|c|c|c|}\hline 0&2&1&0\\\hline 2&0&1&1\\\hline 1&1&1&1\\\hline 0&1&1&2\\\hline\end{array} \qquad \mathbf{C}_{85,4}: \begin{array}{|c|c|c|c|}\hline 2&1&6&2\\\hline 4&4&2&1\\\hline 2&4&2&4\\\hline 4&2&1&4\\\hline\end{array}\ g = 3$$

b: $g = 12$, $x = 52$;

$$\mathbf{C}_{5,4}: \begin{array}{|c|c|c|c|}\hline 0&1&0&0\\\hline 0&0&0&1\\\hline 0&0&0&0\\\hline 0&0&1&0\\\hline\end{array} \qquad \mathbf{C}_{17,4}: \begin{array}{|c|c|c|c|}\hline 0&2&1&0\\\hline 2&0&1&1\\\hline 1&1&1&1\\\hline 0&1&1&2\\\hline\end{array} \qquad \mathbf{C}_{85,4}: \begin{array}{|c|c|c|c|}\hline 4&5&0&2\\\hline 2&2&2&4\\\hline 4&2&4&2\\\hline 2&2&5&2\\\hline\end{array}\ g = 12$$

Using Theorem 1, we can easily derive the analogue of Lemma 1 for the domains $\mathbf{Z}_{pq}$:

LEMMA 4.

(1) $(i, j)_{pq} = (i + ne, j + me)_{pq}$ *for all* $m, n \in \mathbf{Z}$,

(2) $(i, j)_{pq} = (e - i, j - i)_{pq}$

(3) $$(i, j)_{pq} = \begin{cases} (j, i)_{pq} & \text{if } ff' \text{ is odd} \\ \left(j + \frac{e}{2}, i + \frac{e}{2}\right)_{pq} & \text{if } ff' \text{ is even.} \end{cases}$$

(4) $\sum_{j=0}^{e-1} (i, j)_{pq} = \dot{M} + \delta_{pq,i}$ *where* $e\dot{M} = (p - 2)(q - 2) - 1$ *and*

$$\delta_{pq,i} = \sum_{k=0}^{e-1} \theta_{p,k+i}\theta_{q,k}\,.$$

Direct computation shows that

$$\delta_{pq,i} = \begin{cases} 1 & \text{if } ff' \text{ odd}, \quad i = 0 \\ 1 & \text{if } ff' \text{ even}, \quad i = \frac{e}{2} \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} 1 & \text{if } -1 \in C_{pq,k} \\ 0 & \text{otherwise.} \end{cases}$$

The *periods* of $\mathbf{Z}_{pq}$ and g are defined to be

$$\eta_{pq,k} = \sum_{a \in C_{pq,k}} \lambda_{pq}^{a} = \sum_{s=0}^{d-1} \lambda_{pq}^{g^s x^k}$$

for $k = 0, 1, \ldots, e - 1$; clearly,

$$\sum_{k=0}^{e-1} \eta_{pq,k} = 1.$$

Here, as in $\mathbf{Z}_p$, there is an intimate connection between the products of the periods and the cyclotomic numbers; the following lemma (see [2], p. 98) is the domain-analogue of Lemma 2.

LEMMA 5.

$$\eta_{pq,0}\eta_{pq,k} = \sum_{j=0}^{e-1} (k,j)\,\eta_{pq,j} - 2ff' + \left(\frac{pq-1}{e}\right)\delta_{pq,k}; \qquad (k = 0, 1, \ldots, e-1).$$

When e divides none of m, n, nor $m+n$, we introduce two arithmetic functions on $\mathbf{Z}_{pq}$:

$$F_{pq}(\lambda_e^m) = \sum_{k=0}^{e-1} \lambda_e^{mk}\eta_{pq,k}$$

and

$$R_{pq}(m,n) = \sum_{k=0}^{e-1} \lambda_e^{mk} \sum_{h=0}^{e-1} \lambda_e^{-(m+n)h}(k,h)_{pq}\,.$$

We have shown in [6] that Theorem 1 implies that these functions split over the summand fields, as indicated in the following lemma.

LEMMA 6.

(1) *If* $q \in C_{p,\alpha}$ *and* $p \in C_{q,\beta}$, *then*

$$F_{pq}(\lambda_e^m) = \lambda_e^{m(\beta-\alpha)} F_p(\lambda_e^m)\, F_q(\lambda_e^{-m}).$$

(2) $R_{pq}(m,n) = R_p(m,n)\, R_q(-m,-n)$.

The many well-known properties of these function now follow directly from Lemmas 3 and 6; we state the two of interest to our discussion below.

COROLLARY 1.

(1) $R_{pq}(m,n) = \dfrac{F_{pq}(\lambda_e^m)\, F_{pq}(\lambda_e^n)}{F_{pq}(\lambda_e^{m+n})}$.

(2) *If* ℓ *and* ℓ' *are the natural numbers determined by* $g^{\ell} \equiv 2 \pmod p$ *and* $g^{\ell'} \equiv 2 \pmod q$, *then*

$$F_{pq}(-1)\, F_{pq}(\lambda_e^{2k}) = \lambda_e^{2(\ell-\ell')k} F_{pq}(\lambda_e^{k})\, F_{pq}(-\lambda_e^{k}).$$

The significant feature about the above approach is that all results concerning the domain structure were derived entirely within the structures of of the finite fields, and then "patched" together *via* Theorem 1. We have shown in [6] that a direct generalization of Theorem 1 obtains for all the domains $\mathbf{Z}_N$ with $N = \prod_{i=1}^{s} p_i$, and consequently for $GD(\prod_{i=1}^{s} p_i^{\alpha_i})$ (using [2]) and $\mathbf{Z}_{\prod_{i=1}^{s} p_i^{\alpha_i}}$ (using [3]). In the next section we prove the analogue of Theorem 1 for $\mathbf{Z}_{pqr}$, and explicitly derive the class-structure results for these domains.

4. The Galois Domains $GD(p^\alpha q^\beta r^\gamma)$

The recent interest in equations on and the structure of the domains $GD(p^\alpha q^\beta r^\gamma)$ stems from the concluding remarks in [5], where the number of times that an element of the maximal cyclic subgroup of $\mathbf{Z}_{pqr}$ is immediately followed by another such element was explicitly determined (using characters) in the very special case

$$e = \text{l.c.m.}\langle \text{g.c.d.}(p-1, q-1), \text{g.c.d.}(p-1, r-1), \text{g.c.d.}(q-1, r-1)\rangle = 2$$

(when the maximal cyclic subgroup is unique). A complete determination of all the cyclotomic numbers for this case was subsequently done in [7] by a purely algebraic technique, and the method developed in [5] was extended to other specialized domains in [8]. Each of these approaches depends heavily upon an analysis of the structure of the domain; here, as in the case for $GD(p^\alpha q^\beta)$, our analysis is carried out in the summand fields.

We now change our notation slightly, to facilitate the subsequent exposition; since several constants will be associated with each of the three distinct primes involved, it will be convenient to relate these *via* the subscript notation. To that end, let $p_0 = ef_0 + 1$, $p_1 = ef_1 + 1$ and $p_2 = ef_2 + 1$, with f_0, f_1, and f_2 pairwise relatively prime, and for $A_0 \subset \mathbf{Z}_{p_0}$, $A_1 \subset \mathbf{Z}_{p_1}$ and $A_2 \subset \mathbf{Z}_{p_2}$ define the class product

$$A_0A_1A_2 = \{p_1p_2a_0 + p_0p_2a_1 + p_0p_1a_2 (\bmod p_0p_1p_2) : a_0 \in A_0, a_1 \in A_1, a_2 \in A_2\},$$

so that

$$\mathcal{M}_{p_0p_1p_2} = \sum_{i,j,k=0}^{e-1} C_{p_0,i}C_{p_1,j}C_{p_2,k}.$$

Further, if m_0, m_1, and m_2 are integers such that

$$p_1p_2m_0 + p_0p_2m_1 + p_0p_1m_2 = 1,$$

define the natural numbers α_0, α_1, and α_2 by

$$m_0 \in C_{p_0,\alpha_0}, \qquad m_1 \in C_{p_1,\alpha_1}, \qquad m_2 \in C_{p_2,\alpha_2}$$

so that

$$1 \in C_{p_0,\alpha_0} C_{p_1,\alpha_1} C_{p_2,\alpha_2} \subset \mathscr{M}_{p_0p_1p_2}.$$

Finally, define the classes

$$C_{p_0p_1p_2,i,j} = \sum_{k=0}^{e-1} C_{p_0,(\alpha_0+i)+k} C_{p_1,(\alpha_1+j)+k} C_{p_2,\alpha_2+k}; \qquad i,j = 0, 1,\dots, e-1.$$

We are now able to realize the *cyclotomic classes* for $\mathbf{Z}_{p_0p_1p_2}$ as sums of products of the corresponding classes in the summand fields.

LEMMA 6. *Let g_0, g_1, and g_2 be generators of $\mathbf{Z}_{p_0}$, $\mathbf{Z}_{p_1}$, and $\mathbf{Z}_{p_2}$, respectively, and let $g \in \mathbf{Z}_{p_0p_1p_2}$ be the corresponding common primitive root of p_0, p_1, and p_2. Define x_0 and y_1 modulo $p_0p_1p_2$ as follows:*

$$x_0 \equiv \begin{cases} g_0 \pmod{p_0} \\ 1 \pmod{p_1p_2} \end{cases} \qquad y_1 \equiv \begin{cases} g_1 \pmod{p_1} \\ 1 \pmod{p_0p_2}. \end{cases}$$

Then, if $d = ef_0f_1f_2$, we have that

$$C_{p_0p_1p_2,i,j} = \{g^s x_0{}^i y^j{}_1 \pmod{p_0p_1p_2} : s = 0, 1,\dots, d-1\}$$

for $i, j = 0, 1,\dots, e-1$.

PROOF. Clearly $C_{p_0p_1p_2,i,j}$ consists of d elements, distinct modulo $p_0p_1p_2$. Further, there exist natural numbers s, t, and u such that

$$1 \equiv p_1p_2g_0^{es+\alpha_0} + p_0p_2g_1^{et+\alpha_1} + p_0p_1g_2^{eu+\alpha_2} \pmod{p_0p_1p_2}.$$

Hence

$$g \equiv p_1p_2g_0^{es+(\alpha_0+1)} + p_0p_2g_1^{et+(\alpha_1+1)} + p_0p_1g_2^{eu+(\alpha_2+1)} \pmod{p_0p_1p_2}$$

is an element of $C_{p_0,\alpha_0+1}C_{p_1,\alpha_1+1}C_{p_2,\alpha_2+1} \subseteq C_{p_0p_1p_2,0,0}$, by definition. Further,

$$x_0 \equiv p_1p_2g_0^{es+(\alpha_0+1)} + p_0p_2g_1^{et+\alpha_1} + p_0p_1g_2^{eu+\alpha_2} \pmod{p_0p_1p_2}$$

$$y_1 \equiv p_1p_2g_0^{es+\alpha_0} + p_0p_2g_1^{et+(\alpha_1+1)} + p_0p_1g_2^{eu+\alpha_2} \pmod{p_0p_1p_2},$$

and so

$$g^s x_0 \in C_{p_0p_1p_2,1,0} \qquad \text{and} \qquad g^t y_1 \in C_{p_0p_1p_2,0,1}$$

for all s and t. Thus the lemma is proved. ∎

Using Lemma 6, we define the classes $C_{p_0p_1p_2,i,j}$ to be the cyclotomic classes.

We now define the *periods*

$$\eta_{p_0p_1p_2,i,j} = \sum_{b \in C_{p_0p_1p_2,i,j}} \lambda^b_{p_0p_1p_2}; \qquad i,j = 0, 1, \ldots, e-1,$$

so that

$$\sum_{i,j=0}^{e-1} \eta_{p_0p_1p_2,i,j} = -1.$$

As before, we define the *cyclotomic numbers* $(i, j; m, n)_{p_0p_1p_2}$ to be the number of solutions of the equation

$$Z_{i,j} + 1 \equiv Z_{m,n} \pmod{p_0p_1p_2}; \qquad Z_{i,j} \in C_{p_0p_1p_2,i,j}; \qquad Z_{m,n} \in C_{p_0p_1p_2,m,n};$$

i.e., the number of ordered pairs (s, t); $0 \leqslant s, t \leqslant d-1$, such that

$$g^s x_0{}^i y_1{}^j + 1 \equiv g^t x_0{}^m y_1{}^n \pmod{p_0p_1p_2}.$$

Then, analogous to Lemmas 2 and 5, we find that the products of the periods for $\mathbf{Z}_{p_0p_1p_2}$ are related to the corresponding cyclotomic numbers by the following formula.

LEMMA 7.

$$\begin{aligned}
\eta_{p_0p_1p_2,0,0}\, \eta_{p_0p_1p_2,i,j} = & \sum_{\ell,m=0}^{e-1} (i, j; \ell, m)_{p_0p_1p_2}\, \eta_{p_0p_1p_2,\ell,m} \\
& + \Bigg\{ f_0 \sum_{t=0}^{e-1} \theta_{p_0,i+t} \sum_{m,n=0}^{e-1} (j+t, m)_{p_1} (t, n)_{p_2}\, \eta_{p_1p_2,m-n} \\
& + f_1 \sum_{t=0}^{e-1} \theta_{p_1,j+t} \sum_{\ell,n=0}^{e-1} (i+t, \ell)_{p_0} (t, n)_{p_2}\, \eta_{p_0p_2,\ell-n} \\
& + f_2 \sum_{t=0}^{e-1} \theta_{p_2,t} \sum_{\ell,m=0}^{e-1} (i+t, \ell)_{p_0} (j+t, m)_{p_1}\, \eta_{p_0p_1,\ell-m} \\
& - f_0 f_1 f_2 (\delta_{p_0p_1,i-j} + \delta_{p_0p_2,i} + \delta_{p_1p_2,j}) \\
& + (d + f_0 f_1 + f_0 f_2 + f_1 f_2)\, \zeta_{p_0p_1p_2,i,j} \Bigg\}, \\
= & \sum_{\ell,m=0}^{e-1} (i, j; m, n)_{p_0p_1p_2}\, \eta_{p_0p_1p_2} + A_{i,j},
\end{aligned}$$

where the above constitutes a definition of $A_{i,j}$, *a polynomial in* λ_n*'s, for n any proper divisor of* $p_0p_1p_2$ *(the terms of which arise for those t such that* $g^t x_0{}^i y_1{}^j + 1$ *is a nonunit in* $\mathbf{Z}_{p_0p_1p_2}$*), and*

$$\zeta_{p_0p_1p_2,i,j} = \begin{cases} 1 & \text{if } f_0f_1f_2 \text{ is odd and } i = j = 0 \\ 1 & \text{if } f_0 \text{ is even and } i = \frac{e}{2}, \quad j = 0 \\ 1 & \text{if } f_1 \text{ is even and } i = 0, \quad j = \frac{e}{2} \\ 1 & \text{if } f_2 \text{ is even and } i = j = \frac{e}{2} \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. The proof is entirely similar to the proof of Lemma 5, (see [2], p. 98) upon noting that

$$\zeta_{p_0p_1p_2,i,j} = \sum_{t=0}^{e-1} \theta_{p_0,i+t}\theta_{p_1,j+t}\theta_{p_2,t} = \begin{cases} 1 & \text{if } \quad -1 \in C_{p_0p_1p_2,i,j} \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\delta_{p_0p_1,i-j} = \sum_{t=0}^{e-1} \theta_{p_0,i+t}\theta_{p_1,j+t}. \qquad \blacksquare$$

We now prove an analogue of Theorem 1 for the domains $\mathbf{Z}_{p_0p_1p_2}$, including a complete statement of the situation.

THEOREM 2. *Let* $p_0 = ef_0 + 1$, $p_1 = ef_1 + 1$, *and* $p_2 = ef_2 + 1$ *be distinct odd primes, with* f_0, f_1, *and* f_2 *pairwise relatively prime, let* g_0, g_1 *and* g_2 *be generators of* $\mathbf{Z}_{p_0}$, $\mathbf{Z}_{p_1}$, *and* $\mathbf{Z}_{p_2}$, *respectively, and g the corresponding common primitive root of* p_0, p_1, *and* p_2 *modulo* $p_0p_1p_2$. *Let* C_n; $(n = p_0, p_1,$ *or* $p_2)$ *be the cyclotomic classes,* $\mathbf{C}_{n,e}$ *the cyclotomic matrices, and let* $C_{p_0p_1p_2,i,j}$, *be the cyclotomic classes in* $\mathbf{Z}_{p_0p_1p_2}$. *Then, if P and Q are the permutation matrices*

$$P = \operatorname{Circ}\overbrace{(0, 1, 0, \ldots, 0)}^{e} = \left\{\begin{array}{c|c} 0 & I_{e-1} \\ \hline 1 & 0 \end{array}\right\},$$

$$Q = \operatorname{Circ}\overbrace{(0, 0, \ldots, 0, 1)}^{e} = \left\{\begin{array}{c|c} 0 & 1 \\ \hline I_{e-1} & 0 \end{array}\right\},$$

we have

$$(i, j; \ell, m)_{p_0p_1p_2} = (P^i\mathbf{C}_{p_0,e}Q^\ell) \cdot (P^j\mathbf{C}_{p_1,e}Q^m) \cdot \mathbf{C}_{p_1e}$$

for all $i, j, \ell, m = 0, 1, \ldots, e-1$, *and this defines* $\mathbf{C}_{p_0p_1p_2,e}$. *Note that here, if*

$$A^{(n)} = \{[a_{i,j}^{(n)}] : i, j = 0, 1, \ldots, e-1\} \qquad n = 0, 1, 2,$$

then

$$A^{(0)} \cdot A^{(1)} \cdot A^{(2)} = \sum_{i,j=0}^{e-1} a_{i,j}^{(0)} a_{i,j}^{(1)} a_{i,j}^{(2)}.$$

PROOF. We proceed to give an alternate evaluation of $\eta_{p_0p_1p_2,0,0}\eta_{p_0p_1p_2,i,j}$ based on Lemma 6. Clearly, in terms of the η's, Lemma 6 says no more than that

$$\eta_{p_0p_1p_2,i,j} = \sum_{t=0}^{e-1} \eta_{p_0,\alpha_0+i+t}\eta_{p_1,\alpha_1+j+t}\eta_{p_2,\alpha_2+t}$$

for all $i, j = 0, 1, \ldots, e-1$. Hence

$$\eta_{p_0p_1p_2,0,0}\eta_{p_0p_1p_2,i,j}$$

$$= \left(\sum_{s=0}^{e-1} \eta_{p_0,\alpha_0+s}\eta_{p_1,\alpha_1+s}\eta_{p_2,\alpha_2+s}\right)\left(\sum_{t=0}^{e-1} \eta_{p_0,\alpha_0+i+t}\eta_{p_1,\alpha_1+j+t}\eta_{p_2,\alpha_2+t}\right)$$

$$= \sum_{s,t=0}^{e-1} \left(\eta_{p_0,\alpha_0+s}\eta_{p_0,(\alpha_0+s)+(i+t)}\right)\left(\eta_{p_1,\alpha_1+s}\eta_{p_1,(\alpha_1+s)+(j+t)}\right)\left(\eta_{p_2,\alpha_2+s}\eta_{p_2,(\alpha_2+s)+t}\right)$$

$$= \sum_{s,t=0}^{e-1} \left\{\left(\sum_{\ell=0}^{e-1} (i+t, \ell)_{p_0}\, \eta_{p_0,\alpha_0+s+\ell} + f_0\theta_{p_0,i+t}\right)\right.$$

$$\left.\times \left(\sum_{m=0}^{e-1} (j+t, m)_{p_1}\, \eta_{p_1,\alpha_1+s+m} + f_1\theta_{p_1,j+t}\right)\left(\sum_{n=0}^{e-1} (t, n)_{p_2}\, \eta_{p_2,\alpha_2+s+n} + f_2\theta_{p_2,t}\right)\right\}$$

$$= \sum_{s,t=0}^{e-1} \left(\sum_{\ell,m,n=0}^{e-1} (i+t, \ell)_{p_0} (j+t, m)_{p_1} (t, n)_{p_2}\, \eta_{p_0,\alpha_0+s+\ell}\eta_{p_1,\alpha_1+s+m}\eta_{p_2,\alpha_2+s+n}\right) + A'_{i,j}.$$

where, since every term of the first expression on the right is a constant times a primitive $p_0p_1p_2$nd root of unity, and every term of $A'_{i,j}$ is a constant times $\lambda^n_{p_0p_1p_2}$ [where g.c.d. $(n, p_0p_1p_2) > 1$], we must have $A'_{i,j} = A_{i,j}$ of Lemma 7.

A simple computation shows, in fact, that the seven summations occurring in $A'_{i,j}$ are termwise identical to those appearing in $A_{i,j}$.

But, we also have that

$$\sum_{s,t,\ell,m,n=0}^{e-1} (i+t,\ell)_{p_0}(j+t,m)_{p_1}(t,n)_{p_2}\,\eta_{p_0,\alpha_0+s+\ell}\eta_{p_1,\alpha_1+s+m}\eta_{p_2,\alpha_2+s+n}$$

$$= \sum_{t,\ell,m,n=0}^{e-1} (i+t,\ell)_{p_0}(j+t,m)_{p_1}(t,n)_{p_2} \sum_{s=0}^{e-1} \eta_{p_0,\alpha_0+(\ell-n)+s}\eta_{p_1,\alpha_1+(m+n)+s}\eta_{p_2,\alpha_2+s}$$

$$= \sum_{t,\ell,m,n=0}^{e-1} (i+t,\ell)_{p_0}(j+t,m)_{p_1}(t,n)_{p_2}\,\eta_{p_0p_1p_2,\ell-n,m-n}$$

$$= \sum_{\ell,m=0}^{e-1}\left(\sum_{t,n=0}^{e-1} (i+t,\ell+n)_{p_0}(j+t,m+n)_{p_1}(t,n)_{p_2}\right)\eta_{p_0p_1p_2,\ell,m}\,.$$

Hence, comparison of coefficients between the above expression and that obtained in Lemma 7 yields

$$(i,j;\ell,m)_{p_0p_1p_2} = \sum_{t,n=0}^{e-1} (i+t,\ell+n)_{p_0}(j+t,m+n)_{p_1}(t,n)_{p_2}$$

for all $i,j;\ell,m = 0,1,\ldots,e-1$. This is the elementwise formulation of the matrix product defined in the theorem. ∎

COROLLARY.

$$(0,0;0,0)_{p_0p_1p_2} = \mathbf{C}_{p_0,e}\cdot\mathbf{C}_{p_1,e}\cdot\mathbf{C}_{p_2,e}\,.$$

If, for the $(e\times e)$-matrices

$$A^{(n)} = \{[a_{i,j}^{(n)}] : i,j = 0,1,\ldots,e-1\} \qquad n = 0,1,2,$$

we define the product

$$A^{(0)} * A^{(1)} * A^{(2)} = B,$$

where B is the $(e^2\times e^2)$-matrix $[b_{i,j}]$, $i,j = 0,1,\ldots,e^2-1$ defined as follows: if

$$i = ev_1 + u_1 \qquad 0 \leqslant u_1,\ v_1 \leqslant e-1$$

$$j = ev_2 + u_2 \qquad 0 \leqslant u_2,\ v_2 \leqslant e-1,$$

then

$$b_{i,j} = \sum_{t,n=0}^{e-1} a^{(0)}_{u_1+t,u_2+n} a^{(1)}_{v_1+t,v_2+n} a^{(2)}_{t,n};$$

then the conclusion of Theorem 2 may be more compactly written

$$\mathbf{C}_{p_0p_1p_2,e} = \mathbf{C}_{p_0,e} * \mathbf{C}_{p_1,e} * \mathbf{C}_{p_2,e},$$

where the cyclotomic numbers $(i, j; \ell, m)_{p_0p_1p_2}$ are identified with the pairs $(ej + i, em + \ell)_{p_0p_1p_2}$ of $\mathbf{C}_{p_0p_1p_2,e}$. We shall, however, after listing several examples, continue to work with the cyclotomic numbers as ordered quadruples.

We present two examples of Theorem 2; (I) $p_0p_1p_2 = 385$, $e = 2$, and (II) $p_0p_1p_2 = 1105$, $e = 4$. The matrices $\mathbf{C}_{p_0p_1p_2,e}$ were constructed directly from the domains $\mathbf{Z}_{385}$ and $\mathbf{Z}_{1105}$, in order to verify Theorem 2 in these cases.

EXAMPLES.

(I) $p_0p_1p_2 = 385$, $e = 2$; $g = 17$, $x_0 = 232$, $y_1 = 276$

$p_0 = 5 = 2\cdot2 + 1$, $g_0 = 2$ $p_1 = 7 = 2\cdot3 + 1$, $g_1 = 3$ $p_2 = 11 = 2\cdot5 + 1$, $g_2 = 6$

$C_{5,2}$:

0	1
1	1

$C_{7,2}$:

1	2
1	1

$C_{11,2}$:

2	3
2	2

$C_{385,2}$:

10	6	7	8
10	10	9	9
9	8	9	8
9	7	7	9

$g = 17$

II. $p_0p_1p_2 = 1105$, $e = 4$; $g = 7$, $x_0 = 222$, $y_1 = 1021$

$p_0 = 5 = 4\cdot1 + 1$, $g_0 = 2$ $p_1 = 13 = 4\cdot3 + 1$, $g_1 = 7$ $p_2 = 17 = 4\cdot4 + 1$, $g_2 = 7$

$C_{5,4}$:

0	1	0	0
0	0	0	1
0	0	0	0
0	0	1	0

$C_{13,4}$:

0	0	2	1
1	1	1	0
0	1	0	1
1	1	0	1

$C_{17,4}$:

0	0	1	2
0	2	1	1
1	1	1	1
2	1	1	0

$C_{1105,4}$:

0	2	6	2	2	2	2	0	4	1	2	0	0	2	8	0
3	5	0	1	1	1	6	3	1	1	1	0	2	2	1	1
2	2	2	2	0	2	1	4	0	4	1	2	1	4	1	4
5	0	1	3	3	1	2	1	1	1	0	2	1	1	1	6
3	0	2	1	1	1	0	3	2	0	1	8	1	1	4	1
2	1	6	0	1	2	1	2	2	1	1	6	0	2	2	1
1	3	2	0	1	0	3	1	8	1	1	4	1	0	2	1
0	2	1	3	5	4	3	0	1	2	6	0	1	4	1	0
1	5	1	1	1	1	1	2	3	1	2	2	6	1	0	2
4	0	2	1	1	4	1	1	0	4	1	2	2	1	1	4
5	2	0	2	2	2	1	5	0	0	3	2	1	1	1	3
0	3	0	5	3	2	1	0	0	4	2	0	2	4	3	0
3	2	3	2	1	2	5	1	4	1	2	2	6	0	0	2
3	1	1	0	2	4	1	4	1	2	1	1	0	4	0	2
3	1	1	2	2	0	0	6	1	2	2	1	1	1	1	5
0	1	2	5	6	4	2	0	1	4	1	0	3	1	3	0

$g = 7$

As in the case of the domains $\mathbf{Z}_{p_0 p_1}$, replacement of the generator g by a new generator g^* may no longer leave $C_{p_0 p_1 p_2, 0, 0}$, nor hence any $C_{p_0 p_1 p_2, i, j}$, fixed, and so in general there will be several distinct cyclotomic matrices $\mathbf{C}_{p_0 p_1 p_2, e}$ which cannot be obtained one form the other by permutations. Here we have

$$\phi(p_0 - 1)\,\phi(p_1 - 1)\,\phi(p_2 - 1) = [\phi(e)]^2\,\phi(d),$$

and hence we can show that there are at most $[\phi(e)]^2$ inequivalent cyclotomic matrices definable on $\mathbf{Z}_{p_0 p_1 p_2}$ for a given e; there is no guarantee that there are, in general, at least this many.

As a final example, we remark that the Corollary to Theorem 1 has been applied in [6] to very simply obtain the final result of [5] (mentioned in the introductory paragraph of the present section). This we state below.

LEMMA 8. *Let* $e = 2$ *and*

$$\dot{M} = (p_0 - 2)(p_1 - 2)(p_2 - 2) + p_0 + p_1 + p_2 - 8;$$

then

$$16(0, 0; 0, 0)_{p_0 p_1 p_2} = \begin{cases} \dot{M} + 2(p_0 + p_1 + p_2) - 4 & \textit{if} \quad f_0 f_1 f_2 \quad \textit{is odd} \\ \dot{M} + 2p_0 & \textit{if} \quad f_0 \quad \textit{is even} \\ \dot{M} + 2p_1 & \textit{if} \quad f_1 \quad \textit{is even} \\ \dot{M} + 2p_2 & \textit{if} \quad f_2 \quad \textit{is even.} \end{cases}$$

Note that here there is exactly $[\phi(2)]^2 = 1$ distinct cyclotomic matrix for $\mathbf{Z}_{p_0 p_1 p_2}$, and the entry $(0, 0; 0, 0)_{p_0 p_1 p_2}$ of this matrix is given by the Corollary to Theorem 2.

We now use Theorem 2 to prove an analogue of Lemma 1 for these domains.

LEMMA 9.

(1) $(i + a_1 e, j + a_2 e; \ell + a_3 e, m + a_4 e)_{p_0 p_1 p_2} = (i, j; \ell, m)_{p_0 p_1 p_2}$ *for all*

$$a_1, a_2, a_3, a_4 \in \mathbf{Z}.$$

(2) $(i, j; \ell, m)_{p_0 p_1 p_2} = (e - i, e - j; \ell - i, m - j)_{p_0 p_1 p_2}$.

(3) $(i, j; \ell, m)_{p_0 p_1 p_2}$

$$= \begin{cases} (\ell, m; i, j)_{p_0 p_1 p_2} & \text{if} \quad f_0 f_1 f_2 \quad \text{odd} \\ \left(\ell + \frac{e}{2}, m; i + \frac{e}{2}, j\right)_{p_0 p_1 p_2} & \text{if} \quad f_0 \quad \text{even} \\ \left(\ell, m + \frac{e}{2}; i, j + \frac{e}{2}\right)_{p_0 p_1 p_2} & \text{if} \quad f_1 \quad \text{even} \\ \left(\ell + \frac{e}{2}, m + \frac{e}{2}; i + \frac{e}{2}, j + \frac{e}{2}\right)_{p_0 p_1 p_2} & \text{if} \quad f_2 \quad \text{even.} \end{cases}$$

(4) $$\sum_{\ell, m=0}^{e-1} (i, j; \ell, m)_{p_0 p_1 p_2} = (d - f_0 f_1 - f_0 f_2 - f_1 f_2)$$
$$+ f_2 \delta_{p_0 p_1, i-j} + f_1 \delta_{p_0 p_2, i} + f_0 \delta_{p_1 p_2, j} - \zeta_{p_0 p_1 p_2, i, j}.$$

PROOF.

(1) Obvious.

(2) $(e - i, e - j; \ell - i, m - j)_{p_0 p_1 p_2}$

$$= \sum_{t, n=0}^{e-1} (e - i + t, \ell - i + n)_{p_0} (e - j + t, m - j + n)_{p_1} (t, n)_{p_2}$$

$$= \sum_{t, n=0}^{e-1} (i - t, \ell - t + n)_{p_0} (j - t, m - t + n)_{p_1} (e - t, n - t)_{p_2}$$

$$= \sum_{t, n=0}^{e-1} (i + t, \ell + n)_{p_0} (j + t, m + n)_{p_1} (t, n)_{p_2}$$

$$= (i, j; \ell, m)_{p_0 p_1 p_2}.$$

(3) If $f_0 f_1 f_2$ is odd, then

$$(\ell, m; i, j)_{p_0p_1p_2} = \sum_{t,n=0}^{e-1} (\ell + t, i + n)_{p_0} (m + t, j + n)_{p_1} (t, n)_{p_2}$$

$$= \sum_{n,t=0}^{e-1} (i + n, \ell + t)_{p_0} (j + n, m + t)_{p_1} (n, t)_{p_2}$$

$$= (i, j; \ell, m)_{p_0p_1p_2}.$$

If f_0 is even, then

$$\left(\ell + \frac{e}{2}, m; i + \frac{e}{2}, j\right)_{p_0p_1p_2} = \sum_{t,n=0}^{e-1} \left(\ell + \frac{e}{2} + t, i + \frac{e}{2} + n\right)_{p_0} \times (m + t, j + n)_{p_1} (t, n)_{p_2}$$

$$= \sum_{n,t=0}^{e-1} (i + n, \ell + t)_{p_0} (j + n, m + t)_{p_1} (n, t)_{p_2}$$

$$= (i, j; \ell, m)_{p_0p_1p_2}.$$

The case for f_1 even is entirely similar.

If f_2 is even, then

$$\left(\ell + \frac{e}{2}, m + \frac{e}{2}; i + \frac{e}{2}, j + \frac{e}{2}\right)_{p_0p_1p_2}$$

$$= \sum_{t,n=0}^{e-1} \left(\ell + \frac{e}{2} + t, i + \frac{e}{2} + n\right)_{p_0} \left(m + \frac{e}{2} + t, j + \frac{e}{2} + n\right)_{p_1} (t, n)_{p_2}$$

$$= \sum_{t,n=0}^{e-1} (\ell + t, i + n)_{p_0} (m + t, j + n)_{p_1} \left(t + \frac{e}{2}, n + \frac{e}{2}\right)_{p_2}$$

$$= \sum_{n,t=0}^{e-1} (i + n, \ell + t)_{p_0} (j + n, m + t)_{p_1} (n, t)_{p_2}$$

$$= (i, j; \ell, m)_{p_0p_1p_2}.$$

(4) $$\sum_{\ell,m=0}^{e-1} (i, j; \ell, m)_{p_0p_1p_2} = \sum_{\ell,m=0}^{e-1} \sum_{t,n=0}^{e-1} (i + t, \ell + n)_{p_0} \times (j + t, m + n)_{p_1} (t, n)_{p_2}$$

$$= \sum_{t,n=0}^{e-1} (f_0 - \theta_{p_0,i+t})(f_1 - \theta_{p_1,j+t})(t, n)_{p_2}$$

$$= \sum_{t=0}^{e-1} (f_0 - \theta_{p_0,i+t})(f_1 - \theta_{p_1,j+t})(f_2 - \theta_{p_2,t})$$

$$= d - f_0 f_1 - f_0 f_2 - f_1 f_2 + f_2\, \delta_{p_0 p_1, i-j}$$

$$+ f_1\, \delta_{p_0 p_2, j} + f_0\, \delta_{p_1 p_2, j} - \zeta_{p_0 p_1 p_2, i, j}\,. \quad \blacksquare$$

Finally, a few remarks concerning arithmetic functions on the domains $\mathbf{Z}_{p_0 p_1 p_2}$ are in order. For each pair μ_0, μ_1, with $1 \leqslant \mu_0, \mu_1 \leqslant e-1$, $\mu_0 + \mu_1 \not\equiv 0 \pmod{e}$, and, without loss of generality, g.c.d. $(\mu_0, \mu_1) = 1$, we define

$$F^{(\mu_0,\mu_1)}_{p_0 p_1 p_2}(\lambda_e^{\,m}) = \sum_{i,j=0}^{e-1} \lambda_e^{m(\mu_0 i + \mu_1 j)} \eta_{p_0 p_1 p_2, i, j}$$

and

$$R^{(\mu_0,\mu_1)}_{p_0 p_1 p_2}(m, n) = \sum_{i,k=0}^{e-1} \lambda_e^{n(\mu_0 i + \mu_1 k)} \sum_{j,\ell=0}^{e-1} \lambda_e^{-(m+n)(\mu_0 j + \mu_1 \ell)} (i, k; j, \ell)_{p_0 p_1 p_2},$$

whenever none of m, n, nor $m + n$ is divisible by e. We then have the following analogue of Lemma 6, Part (1).

LEMMA 10.

$$F^{(\mu_0,\mu_1)}_{p_0 p_1 p_2}(\lambda_e^{\,m}) = \lambda_e^{-m[\mu_0\alpha_0 + \mu_1\alpha_1 - (\mu_0+\mu_1)\alpha_2]} F_{p_0}(\lambda_e^{\mu_0 m}) F_{p_1}(\lambda_e^{\mu_1 m}) F_{p_2}(\lambda_e^{-(\mu_0+\mu_1)m}).$$

PROOF.

$$F^{(\mu_0,\mu_1)}_{p_0 p_1 p_2}(\lambda_e^{\,m}) = \sum_{i,j=0}^{e-1} \lambda_e^{m(\mu_0 i + \mu_1 j)} \eta_{p_0 p_1 p_2, i, j}$$

$$= \sum_{i,j=0}^{e-1} \lambda_e^{m(\mu_0 i + \mu_1 j)} \sum_{k=0}^{e-1} \eta_{p_0, \alpha_0 + i + k} \eta_{p_1, \alpha_1 + j + k} \eta_{p_2, \alpha_2 + k}$$

$$= \lambda_e^{-m[\mu_0\alpha_0 + \mu_1\alpha_1 - (\mu_0+\mu_1)\alpha_2]} \left(\sum_{i=0}^{e-1} \lambda_e^{\mu_0 m i} \eta_{p_0, i} \right) \left(\sum_{j=0}^{e-1} \lambda_e^{\mu_1 m j} \eta_{p_1, j} \right)$$

$$\times \left(\sum_{k=0}^{e-1} \lambda_e^{-(\mu_0+\mu_1) m k} \eta_{p_2, k} \right)$$

$$= \lambda_e^{-m[\mu_0\alpha_0 + \mu_1\alpha_1 - (\mu_0+\mu_1)\alpha_2]} F_{p_0}(\lambda_e^{\mu_0 m}) F_{p_1}(\lambda_e^{\mu_1 m}) F_{p_2}(\lambda_e^{-(\mu_0+\mu_1)m}). \quad \blacksquare$$

We remark that, since e is even, one of μ_0, μ_1, or $-(\mu_0+\mu_1)$ must be even; further, $F^{(\mu_0,\mu_1)}_{p_0p_1p_2}(-1)$ is expressible as a constant times the product

$$F_{p_0}[(-1)^{\mu_0}]\,F_{p_1}[(-1)^{\mu_1}]\,F_{p_2}[(-1)^{2e-(\mu_0+\mu_1)}],$$

so no direct analogue of Jacobi's lemma [Lemma 3, Part (2)] holds for these domains.

The R's also split over the summand fields, as in Lemma 6, Part 2, and they are related to the F's as in the Corollary to Lemma 6.

LEMMA 11.

$$R^{(\mu_0,\mu_1)}_{p_0p_1p_2}(m,n)=\frac{F^{(\mu_0,\mu_1)}_{p_0p_1p_2}(\lambda_e^{\,m})\,F^{(\mu_0,\mu_1)}_{p_0p_1p_2}(\lambda_e^{\,n})}{F^{(\mu_0,\mu_1)}_{p_0p_1p_2}(\lambda_e^{m+n})}$$
$$=R_{p_0}(\mu_0m,\mu_0n)\,R_{p_1}(\mu_1m,\mu_1n)$$
$$\times R_{p_2}(-(\mu_0+\mu_1)\,m,-(\mu_0+\mu_1)\,n).$$

PROOF.

$$F^{(\mu_0,\mu_1)}_{p_0p_1p_2}(\lambda_e^{\,m})\,F^{(\mu_0,\mu_1)}_{p_0p_1p_2}(\lambda_e^{\,n})$$
$$=\lambda_e^{-(m+n)[\mu_0\alpha_0+\mu_1\alpha_1-(\mu_0+\mu_1)\alpha_2]}F_{p_0}(\lambda_e^{\mu_0m})\,F_{p_0}(\lambda_e^{\mu_0n})\,F_{p_1}(\lambda_e^{\mu_1m})\,F_{p_1}(\lambda_e^{\mu_1n})$$
$$\times F_{p_2}(\lambda_e^{-(\mu_0+\mu_1)m})\,F_{p_2}(\lambda_e^{-(\mu_0+\mu_1)n})$$
$$=F^{(\mu_0,\mu_1)}_{p_0p_1p_2}(\lambda_e^{m+n})$$
$$\times R_{p_0}(\mu_0m,\mu_0n)\,R_{p_1}(\mu_1m,\mu_1n)\,R_{p_2}(-(\mu_0+\mu_1)\,m,-(\mu_0+\mu_1)\,n).$$

Hence, it remains to show that

$$R^{(\mu_0,\mu_1)}_{p_0p_1p_2}(m,n)=R_{p_0}(\mu_0m,\mu_0n)$$
$$\times R_{p_1}(\mu_1m,\mu_1n)\,R_{p_2}(-(\mu_0+\mu_1)\,m,-(\mu_0+\mu_1)\,n).$$

But,

$$R_{p_0}(\mu_0m,\mu_0n)\,R_{p_1}(\mu_1m,\mu_1n)\,R_{p_2}(-(\mu_0+\mu_1)\,m,-(\mu_0+\mu_1)\,n)$$
$$=\left(\sum_{i=0}^{e-1}\lambda_e^{\mu_0ni}\sum_{j=0}^{e-1}\lambda_e^{-\mu_0(m+n)j}(i,j)_{p_0}\right)\left(\sum_{k=0}^{e-1}\lambda_e^{\mu_1nk}\sum_{\ell=0}^{e-1}\lambda_e^{-\mu_1(m+n)\ell}(k,\ell)_{p_1}\right)$$
$$\times\left(\sum_{s=0}^{e-1}\lambda_e^{-(\mu_0+\mu_1)ns}\sum_{t=0}^{e-1}\lambda_e^{(\mu_0+\mu_1)(m+n)t}(s,t)_{p_2}\right)$$

$$= \sum_{i,k,s=0}^{e-1} \lambda_e^{n[\mu_0 i+\mu_1 k-(\mu_0+\mu_1)s]} \sum_{j,\ell,t=0}^{e-1} \lambda_e^{-(m+n)[\mu_0 j+\mu_1 \ell-(\mu_0+\mu_1)t]}(i,j)_{p_0}(k,\ell)_{p_1}(s,t)_{p_2}$$

$$= \sum_{i,k=0}^{e-1} \lambda_e^{n(\mu_0 i+\mu_1 k)} \sum_{j,\ell=0}^{e-1} \lambda_e^{-(m+n)(\mu_0 j+\mu_1 \ell)}$$

$$\times \sum_{s,t=0}^{e-1} (i+s, j+t)_{p_0}(k+s,\ell+t)_{p_1}(s,t)_{p_2}$$

$$= \sum_{i,k=0}^{e-1} \lambda_e^{n(\mu_0 i+\mu_1 k)} \sum_{j,\ell=0}^{e-1} \lambda_e^{-(m+n)(\mu_0 j+\mu_1 \ell)}(i,k;j,\ell)_{p_0p_1p_2}$$

$$= R_{p_0p_1p_2}^{(\mu_0,\mu_1)}(m,n). \quad \blacksquare$$

By using Lemmas 10 and 11, the many properties of the functions F and R can be derived in this more general setting. For definiteness in what follows, we define

$$F_{p_0p_1p_2}(\lambda_e^m) = F_{p_0p_1p_2}^{(1,1)}(\lambda_e^m)$$

$$R_{p_0p_1p_2}(m,n) = R_{p_0p_1p_2}^{(1,1)}(m,n),$$

and remark that, if we define the more general functions

$$F_{p_0p_1p_2}(\beta_e^m, \gamma_e^n) = \sum_{i,j=0}^{e-1} \beta_e^{mi}\gamma_e^{nj}\eta_{p_0p_1p_2,i,j}$$

and

$$R_{p_0p_1p_2}(m_0, m_1; n_0, n_1)$$

$$= \sum_{i,k=0}^{e-1} \beta_e^{n_0 i}\gamma_e^{n_1 k} \sum_{j,\ell=0}^{e-1} \beta_e^{-(m_0+n_0)j}\gamma_e^{-(m_1+n_1)\ell}(i,k;j,\ell)_{p_0p_1p_2},$$

for primitive eth-roots of unity β_e and γ_e such that $\beta_e\gamma_e \neq 1$, then the methods above will prove results for these functions analogous to Lemmas 10 and 11.

References

1. D. Shanks. "Solved and Unsolved Problems in Number Theory." Vol. I. Spartan, 1962.
2. T. Storer. "Cyclotomy and Difference Sets." Markham, 1967.

3. T. Storer. A note on the arithmetic structure of the integers modulo N. *J. Comb. Theory* (to appear).
4. T. Storer. A complete cyclotomic theory for the integers modulo a product of two distinct odd primes. *Duke Math. J.* (to appear).
5. L. Carlitz and A. L. Whiteman. The number of solutions of some congruences modulo a product of primes. *Trans. Am. Math. Soc.* **112** (1964), 536–552.
6. T. Storer. On the arithmetic structure of Galois domains. *Acta Arith.* (to appear).
7. T. Storer. Cyclotomy in $GD(p^{\alpha}q^{\beta}r^{\gamma})$. *Portugalia Math.* (to appear).
8. P. A. White. The number of solutions of some congruences modulo a product of three primes. *Duke Math. J.* **34** (1967), 1–22.