The Cyclotomic Numbers of Order Eighteen With Applications to Difference Sets*

By L. D. Baumert and H. Fredricksen

1. Introduction. Let $p = ef + 1$ be an odd prime and let g be a fixed primitive root of p. Then the *cyclotomic number* $(k, h)_e$ is the number of solutions x, y of the congruence

$$g^{ex+k} + 1 \equiv g^{ey+h} \pmod{p}, \tag{1.1}$$

where the integers x, y are chosen from $0, 1, \cdots, f-1$. Eq. (1.1) shows that there are at most e^2 distinct cyclotomic numbers $(k, h)_e$ of *order* e. This paper is concerned mainly with determining the $(18)^2$ different $(k, h)_{18}$ associated with a fixed primitive root of a prime of the form $p = 18f + 1$. We also tabulate the cyclotomic numbers of order 9.

Complete solutions to this cyclotomic number problem have been computed for $e = 2 - 6, 8, 10, 12, 14, 16, 20$. For $e = 2 - 6$ see L. E. Dickson [2], for $e = 8$ see E. Lehmer [9], for $e = 10, 12, 16$ see A. L. Whiteman [13], [14], [15] and for $e = 14$ see J. B. Muskat [11]. The case $e = 20$ is due to Muskat and Whiteman jointly and is as yet unpublished.

Cyclotomic numbers play an important role in many number theoretical investigations. The difference sets of M. Hall, Jr. [6] and E. Lehmer [8] provided the impetus for this computation (see Section 5).

Before we turn to the actual calculation, a word about the nature of the problem is in order. Eq. (1.1) shows that $(k, h)_e$ depends not only on the prime p but also on which of the $\phi(p-1)$ primitive roots of p was chosen. The effect of replacing the primitive root g by the primitive root g' ($g' \equiv g^r \pmod{p}$ where $(r, p-1) = 1$) is to permute the $(k, h)_e$ among themselves in accordance with the formula

$$(k, h)_e' = (rk, rh)_e. \tag{1.2}$$

Thus, the set $\{(k, h)_e\}$ is indeterminate in the sense that it can equally well be replaced by $\{(rk, rh)_e\}$, where r is fixed and prime to $p - 1$.

A solution to the cyclotomic number problem is a set of formulas which allow the determination of the $(k, h)_e$ without performing a direct calculation. For example, if $e = 3$ the solution given by Dickson [2, p. 397] is

$$9(0,0)_3 = p - 8 + L, \qquad 18(0,1)_3 = 2p - 4 - L + 9M,$$

$$9(1,2)_3 = p + 1 + L, \qquad 18(0,2)_3 = 2p - 4 - L - 9M,$$

$$(1,0)_3 = (0,1)_3 = (2,2)_3, \qquad (1,1)_3 = (2,0)_3 = (0,2)_3, \qquad (2,1)_3 = (1,2)_3$$

where $4p = L^2 + 27M^2$, $L \equiv 1 \pmod{3}$. In this case the $(k, h)_e$ are uniquely determined except for an ambiguity in the sign of M. The sign of M depends upon the

* This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under contract number NAS 7-100, sponsored by the National Aeronautics and Space Administration.

Received December 6, 1965. Revised August 3, 1966.

primitive root g. In our cases ($e = 9$ and $e = 18$), each cyclotomic number is expressed as a constant plus a linear combination of $p, L, M, c_0, \cdots, c_5$ where $4p = L^2 + 27M^2, L \equiv 7 \pmod 9$ and (β being a primitive 9th root of unity)

$$p = \left(\sum_{i=0}^{5} c_i \beta^i\right)\left(\sum_{i=0}^{5} c_i \beta^{-i}\right)$$

is a factorization of p in the field of 9th roots of unity. For $e = 9$, Tables 1 and 2 provide a complete listing. For $e = 18$, the tables are too large to be included in this paper and have been deposited in the unpublished mathematical tables file maintained by Mathematics of Computation. That portion of the tables for $e = 18$ which is needed to support our difference set calculations is included (see Tables 5 and 6).

Various notations for $(k, h)_e$ will be used in what follows, depending on what form is convenient and clear. These are $(k, h)_e$, (k, h), $(kh)_e$, (kh), kh. For uniformity and for typographical convenience, the letters $A, B, \cdots, H$ are used *in the tables* to represent 10, 11, $\cdots$, 17, respectively.

2. Cyclotomy. This section presents a collection of results which were used in the calculation. In all cases the references given contain a proof of the result, but no attempt was made to cite original sources.

(2.1) $$(k, h) = (k', h') \quad \text{if} \quad k \equiv k', \quad h \equiv h' \pmod e.$$

(2.2) $$\begin{aligned}(k, h) &= (e - k, h - k),\\ &= (h, k) \qquad f \text{ even},\\ &= (h + \tfrac{1}{2}e, k + \tfrac{1}{2}e) \qquad f \text{ odd}, \qquad [2, \text{p. } 394].\end{aligned}$$

(2.3) $$\sum_{h=0}^{e-1} (k, h) = f - n_k \qquad (k = 0, 1, \cdots, e - 1)$$

$$\begin{aligned}\text{where } n_k &= 1 \qquad f \text{ even}, k = 0,\\ &= 1 \qquad f \text{ odd}, k = \tfrac{1}{2}e,\\ &= 0 \qquad \text{otherwise}, \qquad [2, \text{p. } 394].\end{aligned}$$

TABLE 1

Equalities between the $(k, h)_9$

k	h								
	0	1	2	3	4	5	6	7	8
0	00	01	02	03	04	05	06	07	08
1	01	08	12	13	14	15	16	17	12
2	02	12	07	17	24	25	26	24	13
3	03	13	17	06	16	26	36	25	14
4	04	14	24	16	05	15	25	26	15
5	05	15	25	26	15	04	14	24	16
6	06	16	26	36	25	14	03	13	17
7	07	17	24	25	26	24	13	02	12
8	08	12	13	14	15	16	17	12	01

TABLE 2

Cyclotomic numbers of order 9

	Ind 3 ≡ 0 (mod 3)										Ind ≡ 1 (mod 3)										Ind 3 ≡ 2 (mod 3)									
	p	1	L	M	c_0	c_1	c_2	c_3	c_4	c_5	p	1	L	M	c_0	c_1	c_2	c_3	c_4	c_5	p	1	L	M	c_0	c_1	c_2	c_3	c_4	c_5
162(00) =	2	−52	2		108			−54			2	−52	2					−54			2	−52	2					54		
162(01) =	2	−16	−1	9	−12	42	−12	24	−30	24	2	−16	−1	9	24	6	24	−12	−30	−12	2	−16	−1	9	−12	6	−12	−12	6	−12
162(02) =	2	−16	−1	−9	−12	24	42	−12	−12	−12	2	−16	−1	−9	−12	−12	6	24	−12	−12	2	−16	−1	−9	24	−12	6	−12	24	24
162(03) =	2	−16	2		−18			36			2	−16	2		−18			36			2	−16	2		−18			36		
162(04) =	2	−16	−1	9	−12	−12	24	24	42	−12	2	−16	−1	9	24	24	−12	−12	6	−12	2	−16	−1	9	−12	−12	−12	−12	6	24
162(05) =	2	−16	−1	−9	−12	−12	−30	−12	−12	42	2	−16	−1	−9	−12	−12	6	24	24	6	2	−16	−1	−9	24	24	−30	−12	−12	6
162(06) =	2	−16	2		−18			−18			2	−16	2		−18			−18			2	−16	2		−18			−18		
162(07) =	2	−16	−1	9	−12	−30	−12	24	−12	−12	2	−16	−1	9	24	−30	−12	−12	24	24	2	−16	−1	9	−12	6	24	−12	−12	−12
162(08) =	2	−16	−1	−9	−12	−12	−12	−12	24	−30	2	−16	−1	−9	−12	24	−12	24	−12	6	2	−16	−1	−9	24	−12	24	−12	−12	−30
162(12) =	2	2	2			−18	18				2	2	2						18	−18	2	2	2						−18	18
162(13) =	2	2	−1	9	6	6	−12	−12	6	6	2	2	−1	9	−12	−12	6	6	24	6	2	2	−1	9	6	6	6	6	24	−12
162(14) =	2	2	−1	−9	6	−12	6	6	6	6	2	2	−1	−9	6	6	24	−12	6	6	2	2	−1	−9	−12	6	24	6	−12	−12
162(15) =	2	2	2			18			−18	−18	2	2	2			−18	−18			18	2	2	2				18		18	
162(16) =	2	2	−1	9	6	−12	6	−12	6	6	2	2	−1	9	−12	−12	6	6	−12	−12	2	2	−1	9	6	−30	−12	6	6	6
162(17) =	2	2	−1	−9	6	6	−12	6	6	6	2	2	−1	−9	6	6	−30	−12	−12	24	2	2	−1	−9	−12	−12	−12	6	6	24
162(24) =	2	2	2			−18		18	18		2	2	2			18	18		−18		2	2	2			−18				−18
162(25) =	2	2	−1	9	6	6	6	−12	−12	−12	2	2	−1	9	−12	24	−12	6	−12	6	2	2	−1	9	6	24	6	6	−30	6
162(26) =	2	2	−1	−9	6	6	6	6	−12	−12	2	2	−1	−9	6	−12	6	−12	6	−30	2	2	−1	−9	−12	6	−12	6	6	−12
162(36) =	2	2	2								2	2	2		54						2	2	2			54			−54	

Let $\alpha \neq 1$ be a root of $x^{p-1} = 1$ and define

$$F(\alpha) = \sum_{k=0}^{p-2} \alpha^k \exp(2\pi ijg^k/p)$$

with $j \not\equiv 0 \pmod{p}$. Then if $\alpha = \beta^n$, where β is a *primitive* eth root of unity,

(2.4) $$F(\beta^n)F(\beta^{-n}) = (-1)^{nf}p \quad \text{if} \quad e \nmid n \qquad [2, \text{p. } 395].$$

If e does not divide m, n or $m + n$, then define $R(m, n, \beta)_e$ by

(2.5) $$R(m, n, \beta)_e \equiv \frac{F(\beta^m)F(\beta^n)}{F(\beta^{m+n})} = \sum_{k=0}^{e-1} \beta^{nk} \sum_{h=0}^{e-1} \beta^{-(m+n)h}(k, h) \qquad [2, \text{p. } 396].$$

In the symbol $R(m, n, \beta)_e$ the β and/or the e will be suppressed whenever they are not needed for clarity.

(2.6) $$R(m, n) = R(m', n') \quad \text{if} \quad m \equiv m', \quad n \equiv n' \pmod{e}.$$

(2.7) $$R(n, m) = R(m, n) = (-1)^{nf}R(-m - n, n) \qquad [2, \text{p. } 408].$$

(2.8) $$R(m, n)R(-m, -n) = p \qquad [2, \text{p. } 396].$$

(2.9) $$R(m, n, \beta^j) = R(jm, jn, \beta).$$

(2.10) $$R(dm, dn, \beta)_e = R(m, n, \beta^d)_E,$$

where $e = dE$ and β is a primitive eth root of unity throughout [4, p. 188].

(2.11) $$(k, h)_E = \sum_{r,s=0}^{d-1} (k + rE, h + sE)_e, \quad \text{where} \quad e = dE \qquad [4, \text{p. } 188].$$

(2.12) $F(-1)F(\alpha^2) = \alpha^{2B}F(\alpha)F(-\alpha)$, where $g^B \equiv 2 \pmod{p}$ [2, p. 407].

If $p \equiv 1 \pmod{3}$ is prime and if $\gamma \neq 1$ is a cube root of unity, then

(2.13) $F(\alpha)F(\gamma\alpha)F(\gamma^2\alpha) = \alpha^{-3T}pF(\alpha^3), \quad g^T \equiv 3 \pmod{p}$ [1, (0.9)].

When g is replaced by a new primitive root g^r of p,

(2.14) $R(m, n)$ becomes $R(mr', nr')$, where $rr' \equiv 1 \pmod{e}$ [2, p. 409].

In addition to these general cyclotomic facts, the following specific relations for $e = 3, 6, 9$ will be useful.

(2.15) $$2R(1, 1, \beta)_3 = L + 3M + 6M\beta, \quad \text{where} \quad 4p = L^2 + 27M^2, \quad L \equiv 1 \pmod{3} \qquad [2, \text{p. } 397].$$

(2.16) $$R(1, 1, \beta)_6 = (-1)^f\beta^{4B}R(1, 2, \beta)_6, \qquad R(2, 2, \beta)_6 = \beta^{2B}R(1, 2, \beta)_6 \qquad [2, \text{p. } 408].$$

(2.17) $$2R(3, 3, \beta)_9 = L + 3M + 6\beta^3M, \quad \text{where} \quad 4p = L^2 + 27M^2, \quad L \equiv 7 \pmod{9} \qquad [4, \text{p. } 188].$$

(2.18) $$R(1, 2, \beta)_9 = \beta^{6T}R(1, 1, \beta^2)_9 \qquad [4, \text{p. } 189].$$

3. The Cyclotomic Numbers of Order Nine. In this section Dickson's solution [4] for the $(k, h)_9$ is presented. Actually, it is carried a little further than he did in

that the formulas are all displayed. Furthermore, the calculation of the $(k, h)_9$ is much more manageable than that for the $(k, h)_{18}$. This section will thus serve as a model for the next.

Using (2.2) above, the 81 possible $(k, h)_9$ reduce to just 19 distinct ones—the equalities (2.2) between the various $(k, h)_9$ are displayed in Table 1. Hence, the problem will be solved if 19 independent linear equations involving the (k, h) can be found. Eq. (2.3) provides 5 independent equations of this type. That it can provide no more independent equations follows from Table 1, i.e., from (2.2). Since the primitive 9th roots of unity satisfy

$$x^6 + x^3 + 1 = 0, \tag{3.1}$$

by using (2.5) above, one can write

$$R(1, 1)_9 = \sum_{i=0}^{5} c_i\beta^i, \qquad R(1, 2)_9 = \sum_{i=0}^{5} b_i\beta^i, \tag{3.2}$$

where each c_i, b_i is represented by a linear equation in the $(k, h)_9$. This provides 12 more equations, leaving 2 still to be found. These arise out of the solution of the cyclotomic number problem for $(k, h)_3$—or equivalently from

$$R(3, 3, \beta)_9 = R(1, 1, \beta^3)_3 \tag{3.3}$$

which follows from Eq. (2.10) above. If $p \equiv 1 \pmod 3$ then [2, p. 397] $4p = L^2 + 27M^2$ where $M = (01)_3 - (02)_3$ and $L = 9(00)_3 - p + 8 \equiv 1 \pmod 3$. Now these expressions for M, L can be translated using (2.11) into linear equations involving the $(k, h)_9$. Thus, 19 independent linear equations involving the $(k, h)_9$ have been determined and they can be solved yielding the $(k, h)_9$ in terms of the parameters $L, M, c_0, \cdots, c_5, b_0, \cdots, b_5$, which by (2.15) and (3.3) are all related to the coefficients of $R(m, n)_9$'s. By using (2.18) the b_i can be expressed in terms of the c_i at the expense of introducing the parameter T (= index of 3 to the base g modulo p, abbreviated Ind 3), and splitting the solution into 3 cases depending on the value of $T \pmod 3$. The solution appears as Table 2.

Given a prime $p = 9f + 1$ and an associated primitive root g, the $(k, h)_9$ are determined by Tables 1 and 2, provided the values of $L, M, c_0, \cdots, c_5$ can be determined. The relation $4p = L^2 + 27M^2$, $L \equiv 7 \pmod 9$ determines L uniquely and M except for sign. Dickson notes [4, p. 194] that $(2, 6)_9$ is an integer for only one choice of $\pm M$ unless $M \equiv 0 \pmod 9$. He establishes further a final rule for the determination of M,

$$R(3, 3, \beta)_9R(1, 2, \beta)_9 = \beta^{-6T}R(1, 1, \beta)_9R(1, 2, \beta^2)_9 \tag{3.4}$$

which determines M through use of (2.17). A more symmetric form of this can be derived. Use (2.18) to give

$$R(3, 3, \beta)\beta^{6T}R(1, 1, \beta^2) = \beta^{-6T}R(1, 1, \beta)\beta^{12T}R(1, 1, \beta^4)$$

now multiply through by $R(-2, -2, \beta)$ and use (2.9) on $R(1, 1, \beta^2)$, then apply (2.8) to give

$$pR(3, 3, \beta) = R(1, 1, \beta)R(1, 1, \beta^4)R(-2, -2, \beta).$$

Finally, use (2.6), (2.9) on $R(-2, -2, \beta)$ to yield

$$pR(3, 3, \beta)_9 = R(1, 1, \beta)_9 R(1, 1, \beta^4)_9 R(1, 1, \beta^7)_9 . \tag{3.5}$$

The formulas (3.4) and (3.5) determine M only through a knowledge of $c_0 , \cdots , c_5$, thus depend on a solution of that problem. Actually, if M can be determined by some other method, formulas (3.4) and (3.5) can be used to help determine the c_i as is shown below. If $M \not\equiv 0 \pmod 3$ the sign of M can be determined from

$$\text{Ind } 3 + M \equiv 0 \pmod 3. \tag{3.6}$$

One proof of relation (3.6) is as follows: Using Eqs. (3.3) and (2.15) on $R(3,3)_9$ we find that in terms of cyclotomic numbers

$$M = (01) + (04) + (07) - (02) - (05) - (08) + 2[(13) + (16) + (25) - (14) - (17) - (26)]$$

and $R(1, 2)$ yields

$$b_3 = -(01) - (04) - (07) + (02) + (05) + (08) + (13) + (16) + (25) - (14) - (17) - (26).$$

Thus, $M + b_3 \equiv 0 \pmod 3$. But $b_3 = -c_3 , c_3 - c_6 , c_0$ if $T \equiv 0, 1, 2 \pmod 3$ by (2.18). Thus, since $c_0 \equiv -1$, $c_3 \equiv 0 \pmod 3$ [4, p. 191], this implies the desired relation (3.6).

Eqs. (2.5) and (2.8) show that $R(1, 1)$ (and hence the c_i) comes from a factorization of p in the field of 9th roots of unity. Dickson [4, p. 193] has shown that

$$\left(\sum_{i=0}^{5} c_i \beta^i\right)\left(\sum_{i=0}^{5} c_i \beta^{-i}\right) = p$$

has only 6 solutions in which the first factor is *not* invariant under $\beta \to \beta^4$. These are generated from any one of them by applying the powers of the substitution $\beta \to \beta^2$ and reducing by means of (3.1). These are the only candidates for $R(1, 1, \beta)_9$ and indeed as the primitive root shifts from g to g^r through all the different primitive roots, (2.14) shows that $R(1, 1)$ shifts through the 6 possibilities. Three of these candidates yield $| M |$ and three yield $- | M |$. Thus, the sign of M, if known, can be used with (3.5) to rule out three possible $R(1, 1)$'s.

In practice actually it is often easier to find one possible $R(1, 1)$, generate them all by $\beta \to \beta^2$, determine M by (3.5) or (3.6) and let the fact that all $(k, h)_9$ are integers determine which possible $R(1, 1)$ goes with a particular g.

In connection with the formulas for the $(k, h)_9$, it should be mentioned that the third list is redundant. For if $\text{Ind } 3 \equiv 2 \pmod 3$ for the primitive root g, we may change to another primitive root g^r which has $\text{Ind } 3 \equiv 1 \pmod 3$. Computing the $(k, h)_9$ for g^r and using Eq. (1.2) yields the desired cyclotomic numbers.

4. The Cyclotomic Numbers of Order Eighteen. By use of (2.2) above, the 324 possible $(k, h)_{18}$ are reduced to just 64 distinct ones (see Table 3). Eq. (2.3) provides 10 independent linear equations. The remaining 54 equations come from various $R(m, n)$'s. In order to insure that the equations will be independent, some care must be used in choosing the $R(m, n)$'s. This is done by calling two $R(m, n)$'s

TABLE 3a
Equalities between $(k, h)_{18}$, *f odd*

k	h																	
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0G	0H
1	10	11	12	13	14	15	16	17	18	0A	08	18	1C	1D	1E	1F	1G	1H
2	20	21	22	23	24	25	26	27	1C	0B	18	07	17	27	2E	2F	2G	2H
3	30	31	32	33	34	35	36	2E	1D	0C	1C	17	06	16	26	36	3G	3H
4	40	41	42	43	44	45	3G	2F	1E	0D	1D	27	16	05	15	25	35	45
5	44	51	52	53	51	40	3H	2G	1F	0E	1E	2E	26	15	04	14	24	34
6	33	43	53	63	52	41	30	2H	1G	0F	1F	2F	36	25	14	03	13	23
7	22	32	42	52	53	42	31	20	1H	0G	1G	2G	3G	35	24	13	02	12
8	11	21	31	41	51	43	32	21	10	0H	1H	2H	3H	45	34	23	12	01
9	00	10	20	30	40	44	33	22	11	00	10	20	30	40	44	33	22	11
10	10	0H	1H	2H	3H	45	34	23	12	01	11	21	31	41	51	43	32	21
11	20	1H	0G	1G	2G	3G	35	24	13	02	12	22	32	42	52	53	42	31
12	30	2H	1G	0F	1F	2F	36	25	14	03	13	23	33	43	53	63	52	41
13	40	3H	2G	1F	0E	1E	2E	26	15	04	14	24	34	44	51	52	53	51
14	44	45	3G	2F	1E	0D	1D	27	16	05	15	25	35	45	40	41	42	43
15	33	34	35	36	2E	1D	0C	1C	17	06	16	26	36	3G	3H	30	31	32
16	22	23	24	25	26	27	1C	0B	18	07	17	27	2E	2F	2G	2H	20	21
17	11	12	13	14	15	16	17	18	0A	08	18	1C	1D	1E	1F	1G	1H	10

TABLE 3b
Equalities between $(k, h)_{18}$, *f even*

k	h																	
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0G	0H
1	01	0H	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	1G	12
2	02	12	0G	1G	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	24	13
3	03	13	1G	0F	1F	2F	36	37	38	39	3A	3B	3C	3D	3E	36	25	14
4	04	14	24	1F	0E	1E	2E	3E	48	49	4A	4B	4C	4D	48	37	26	15
5	05	15	25	2F	1E	0D	1D	2D	3D	4D	5A	5B	5C	5A	49	38	27	16
6	06	16	26	36	2E	1D	0C	1C	2C	3C	4C	5C	6C	5B	4A	39	28	17
7	07	17	27	37	3E	2D	1C	0B	1B	2B	3B	4B	5B	5C	4B	3A	29	18
8	08	18	28	38	48	3D	2C	1B	0A	1A	2A	3A	4A	5A	4C	3B	2A	19
9	09	19	29	39	49	4D	3C	2B	1A	09	19	29	39	49	4D	3C	2B	1A
10	0A	1A	2A	3A	4A	5A	4C	3B	2A	19	08	18	28	38	48	3D	2C	1B
11	0B	1B	2B	3B	4B	5B	5C	4B	3A	29	18	07	17	27	37	3E	2D	1C
12	0C	1C	2C	3C	4C	5C	6C	5B	4A	39	28	17	06	16	26	36	2E	1D
13	0D	1D	2D	3D	4D	5A	5B	5C	5A	49	38	27	16	05	15	25	2F	1E
14	0E	1E	2E	3E	48	49	4A	4B	4C	4D	48	37	26	15	04	14	24	1F
15	0F	1F	2F	36	37	38	39	3A	3B	3C	3D	3E	36	25	14	03	13	1G
16	0G	1G	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	24	13	02	12
17	0H	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	1G	12	01

conjugate if one comes from the other by changing the primitive root; see (2.14). Now choose one $R(m, n)$ from each conjugate class and delete duplicates arising from (2.7). This process yields $R(1, 1)$, $R(1, 2)$, $R(1, 3)$, $R(1, 4)$, $R(1, 5)$, $R(1, 9)$, $R(3, 3)$, $R(3, 6)$, $R(6, 6)$, $R(2, 2)$ and $R(2, 4)$ in the case $e = 18$. These $R(m, n)$'s give 6, 6, 6, 6, 6, 6, 2, 2, 2, 6, 6, equations respectively, so the 64 equations could be solved yielding $(k, h)_{18}$ in terms of the 54 parameters introduced by the $R(m, n)$'s. As in Section 3, the number of parameters appearing in the (k, h) can be reduced by splitting the solution into cases and introducing the parameters $B = \text{Ind } 2$ and $T = \text{Ind } 3$. In fact, this process (carried out below) reduces the parameters appear-

ing in the $(k, h)_{18}$ to the same L, M, $c_0, \cdots, c_5$ as appeared in $(k, h)_9$; this might have been anticipated since the same cyclotomic field is involved.

The equation satisfied by the primitive 18th roots of unity is

$$x^6 - x^3 + 1 = 0. \tag{4.1}$$

The relations between the various $R(m, n)$'s are:

$$R(6, 6, \beta)_{18} = R(3, 3, \beta^2)_9 = \frac{L + 3M}{2} + 3M\beta^6, \qquad L \equiv 7 \pmod 9 \tag{4.2}$$

by (2.10), (2.17).

$$R(2, 2, \beta)_{18} = R(1, 1, \beta^2)_9 = \sum_{i=0}^{5} c_i\beta^{2i} = (c_0 - c_3) - c_5 6 + (c_1 - c_4)\beta^2 + c_3\beta^3 + c_2\beta^4 + c_4\beta^5 \tag{4.3}$$

by (2.10), (3.2), (4.1).

$$R(8, 8, \beta)_{18} = R(26, 26, \beta)_{18} = R(2, 2, \beta^{13})_{18} = \sum_{i=0}^{5} c_i\beta^{26i} = (c_0 - c_3) + c_2\beta - c_1\beta^2 + c_3\beta^3 + (c_5 - c_2)\beta^4 + (c_1 - c_4)\beta^5 \tag{4.4}$$

by (2.6), (2.9), (4.3), (4.1).

$$R(1, 1, \beta)_{18} = (-1)^f\beta^{-4B}R(-16, 8, \beta)_{18} = (-1)^f\beta^{-4B}R(8, 8, \beta)_{18} \tag{4.5}$$

by [4, p. 194], (2.6), (2.7).

$$R(1, 4, \beta)_{18} = (-1)^f\beta^{-6B}R(1, 1, \beta)_{18} = \beta^{-10B}R(8, 8, \beta)_{18} \tag{4.6}$$

by [4, p. 194], (4.5).

$$R(1, 9, \beta)_{18} = \beta^{2B}R(1, 1, \beta)_{18} = (-1)^f\beta^{-2B}R(8, 8, \beta)_{18} \tag{4.7}$$

by [4, p. 194], (4.5).

$$R(1, 2, \beta)_{18} = (-1)^f\beta^{-3T}R(1, 4, \beta^5)_{18} = (-1)^f\beta^{-3T-14B}R(8, 8, \beta^5)_{18} = (-1)^f\beta^{-3T-14B}[c_0 + c_4\beta + (c_5 - c_2)\beta^2 - c_3\beta^3 + (c_1 - c_4)\beta^4 + c_2\beta^5] \tag{4.8}$$

by [4, p. 194], (4.6), (4.4), (4.1).

$$R(2, 4, \beta)_{18} = R(1, 2, \beta^2)_9 = \beta^{12T}R(1, 1, \beta^4)_9 = \beta^{12T}\sum_{i=0}^{5} c_i\beta^{4i} = \beta^{12T}[c_0 + c_4\beta + (c_5 - c_2)\beta^2 - c_3\beta^3 + (c_1 - c_4)\beta^4 + c_2\beta^5] \tag{4.9}$$

by (2.10), (2.18), (3.2), (4.1).

$$R(1, 5, \beta)_{18} = (-1)^f\beta^{6B}R(2, 4, \beta)_{18} = (-1)^f\beta^{6B+12T}[c_0 + c_4\beta + (c_5 - c_2)\beta^2 - c_3\beta^3 + (c_1 - c_4)\beta^4 + c_2\beta^5] \tag{4.10}$$

by [4, p. 195], (4.9).

Dickson [4, p. 196] related $R(1, 3)_{18}$ with $R(6, 6)_{18}$ but gave no proof and left an ambiguity of sign which we resolve here.

$$\frac{R(1,3)}{R(6,6)} = \frac{F(\beta)F(\beta^3)F(\beta^{12})}{F(\beta^4)F(\beta^6)F(\beta^6)} = \frac{\beta^{-6B}F(\beta)F(\beta^9)}{F(\beta^4)F(\beta^6)} = \frac{\beta^{-6(B+T)}pF(\beta)F(\beta^9)}{\beta^{-6T}pF(\beta^4)F(\beta^6)}$$

by (2.5), (2.12)

$$= \frac{\beta^{-6(B+T)}pF(\beta)F(\beta^9)}{F(\beta^4)F(\beta^8)F(\beta^{14})F(\beta^2)} = \frac{\beta^{-6(B+T)}F(\beta)F(\beta^9)}{F(\beta^2)F(\beta^8)}$$

$$= \beta^{-6(B+T)}\frac{R(1,9)}{R(2,8)} = \beta^{-4B-6T}\frac{R(1,1)}{R(2,8)} = (-1)^f\beta^{-8B-6T}$$

by (2.13), (2.4), (2.5), [4, p. 195].

Thus,

(4.11) $$R(1,3,\beta)_{18} = (-1)^f\beta^{-8B-6T}R(6,6,\beta)_{18}$$

$$= (-1)^f\beta^{-8B-6T}\left[\frac{L+3M}{2} + 3M\beta^6\right] \quad \text{by (4.2).}$$

(4.12) $$R(3,3,\beta)_{18} = R(1,1,\beta^3)_6 = (-1)^{3f}\beta^{12B}R(1,2,\beta^3)_6$$

$$= (-1)^f\beta^{6B}R(2,2,\beta^3)_6 \quad \text{by (2.10), (2.16)}$$

$$= (-1)^f\beta^{6B}R(1,1,\beta^6)_3 = (-1)^f\beta^{6B}\left[\frac{L+3M}{2} + 3M\beta^6\right]$$

by (2.10), (2.15).

(4.13) $$R(3,6,\beta)_{18} = R(1,2,\beta^3)_6 = \beta^{-6B}R(2,2,\beta^3)_6 = \beta^{-6B}R(1,1,\beta^6)_3$$

by (2.10), (2.16).

$$= \beta^{-6B}\left[\frac{L+3M}{2} + 3M\beta^6\right] \quad \text{by (2.15).}$$

Thus, all $R(m, n)$'s are expressed in terms of L, M, $c_0, \cdots, c_5$ and $R(8, 8)$. This implies by (4.4) that they are all expressed in terms of $L, M, c_0, \cdots, c_5$ as promised above.

The introduction of B, T into the equations determining the $(k, h)_{18}$ requires that the solution be split into cases. An examination of Eqs. (4.2), $\cdots$, (4.13) shows that B need be determined only modulo 9 and T modulo 6. This yields 54 possible cases. A reduction in the number of cases follows from the fact that 3 is not a quadratic residue of a prime of the form $36f' + 19$; thus, $T \equiv 1, 3, 5 \pmod 6 \equiv$

TABLE 4

Classes of index pairs; $B \equiv$ Ind 2 (mod 9), $T \equiv$ Ind 3 (mod 3)

g^r	B	T	B	T	B	T	B	T	B	T	B	T	B	T	B	T
$r \equiv 1$ (18)	0	0	0	1	1	0	1	1	1	2	3	0	3	1	3	2
$r \equiv 5$ (18)	0	0	0	2	2	0	2	2	2	1	6	0	6	2	6	1
$r \equiv 7$ (18)	0	0	0	1	4	0	4	1	4	2	3	0	3	1	3	2
$r \equiv 11$ (18)	0	0	0	2	5	0	5	2	5	1	6	0	6	2	6	1
$r \equiv 13$ (18)	0	0	0	1	7	0	7	1	7	2	3	0	3	1	3	2
$r \equiv 17$ (18)	0	0	0	2	8	0	8	2	8	1	6	0	6	2	6	1

TABLE 5

The cyclotomic numbers of order 18, *f odd, for* Ind 2 ≡ 0 (mod 9) *and* Ind 3 ≡ 1 (mod 3)

	P	1	L	M	C_0	C_1	C_2	C_3	C_4	C_5
648(00) =	2	−70	2	54	36			−72		
648(01) =	2	2	−10	36	−48	−30	96	24	−30	−30
648(02) =	2	2	−4	−18	12	−42	−6	−24	−60	−24
648(03) =	2	2	−16		36			90		
648(04) =	2	2	14	−36	48	12	−6	−24	−6	30
648(05) =	2	2	8	18	−12	−12	6	24	6	−30
648(06) =	2	2	−16		36			90		
648(07) =	2	2	−10	36	−48	−30	−66	24	60	96
648(08) =	2	2	−4	−18	12	102	−24	−24	−42	30
648(09) =	2	2	2	−162	−108					
648(0A) =	2	2	14	−36	48	−6	−24	−24	−6	−6
648(0B) =	2	2	8	18	−12	6	−30	24	−12	24
648(0C) =	2	2	20	108	−36			18		
648(0D) =	2	2	−10	36	−48	60	−30	24	−30	−66
648(0E) =	2	2	−4	−18	12	−60	30	−24	102	−6
648(0F) =	2	2	−16		36			−126		
648(0G) =	2	2	14	−36	48	−6	30	−24	12	−24
648(0H) =	2	2	8	18	−12	6	24	24	6	6
648(10) =	2	−34	−4	18	48	30	12	−24	−42	−6
648(11) =	2	−34	−4	−18	−24	−6	−24	48	−6	−6
648(12) =	2	2	2			36	36			−36
648(13) =	2	2	−4	−36	−24	−6	−24	12	30	66
648(14) =	2	2	5	63	−6	−6	30	12	−24	12
648(15) =	2	2	2			−36	−36		36	
648(16) =	2	2	−4	−36	−24	−24	−42	12	30	30
648(17) =	2	2	−13	9	30	−24	−42	−60	−42	−6
648(18) =	2	2	2			36	36			−36
648(1C) =	2	2	−4	72	−24	−42	48	12	30	−6
648(1D) =	2	2	5	−45	−6	−6	30	12	12	−24
648(1E) =	2	2	2						−36	36
648(1F) =	2	2	−4	−36	−24	−24	66	12	−6	−42
648(1G) =	2	2	5	63	−6	−24	−42	12	30	30
648(1H) =	2	2	2			−36	−36		36	
648(20) =	2	−34	−4	−18	−24	−6	30	48	12	−24
648(21) =	2	2	2			−36	−36		36	
648(22) =	2	−34	−4	18	48	−42	−6	−24	12	12
648(23) =	2	2	−1	−63	6	60	−30	−12	−30	42
648(24) =	2	2	2						−36	36
648(25) =	2	2	8	36	24	42	6	−12	−12	−12
648(26) =	2	2	5	−45	−6	−6	−24	12	−6	−6
648(27) =	2	2	2			36	36			−36
648(2E) =	2	2	−4	−36	−24	−6	30	12	−24	12
648(2F) =	2	2	−1	−63	6	−30	−12	−12	−30	−30
648(2G) =	2	2	2			36	36			−36
648(2H) =	2	2	8	36	24	−30	−12	−12	42	6
648(30) =	2	−34	2	−54	−36			18		
648(31) =	2	2	−4	−36	−24	30	12	12	−6	−42
648(32) =	2	2	5	−45	−6	12	−6	12	−6	30
648(33) =	2	−34	20		−72			−18		
648(34) =	2	2	−4	72	−24	12	−6	12	−42	−42
648(35) =	2	2	−13	9	30	−42	48	−60	66	−42
648(36) =	2	2	11	−27	90			−18		
648(3G) =	2	2	−4	72	−24	30	−42	12	12	48
648(3H) =	2	2	−13	9	30	66	−6	−60	−24	48
648(40) =	2	−34	−4	18	48	12	−6	−24	30	−6
648(41) =	2	2	−1	−63	6	−30	42	−12	60	−12
648(42) =	2	2	2						−36	36
648(43) =	2	2	8	36	24	−12	6	−12	−30	6
648(44) =	2	−34	−4	−18	−24	12	−6	48	−6	30
648(45) =	2	2	2						−36	36
648(51) =	2	2	2			−36	−36		36	
648(52) =	2	2	−4	−36	−24	30	−42	12	−24	−24
648(53) =	2	2	5	63	−6	30	12	12	−6	−42
648(63) =	2	2	−25	81	−54			54		

1, 0, 2 (mod 3) for f odd. Thus, there are 27 remaining possibilities, of which a number are redundant in that they can be derived from others by changing the primitive root and using (1.2). Thus, all the 27 possibilities for odd f appear among the 8 classes of Table 4. The primes 2971, 127, 271, 19, 163, 307, 739, 811 are (in order) the smallest primes belonging to these classes [7, pp. 216–267].

Formulas for the $(k, h)_{18}$ are given in Table 5 for the case $B \equiv 0 \pmod 9$, $T \equiv 1 \pmod 3$. For the other index pairs B, T we list only those (k, h) used in Section

TABLE 6

Selected cyclotomic numbers of order 18, f odd

Ind 2 (mod 9)	Ind 3 (mod 3)	648 $(k, h)_{18}$	P	1	L	M	c_0	c_1	c_2	c_3	c_4	c_5
0	0	648(3, 0) =	2	−34	2	54	−36			18		
0	0	648(6, 0) =	2	−34	2	−54	−36			18		
3	0	648(1, 0) =	2	−34	−4	18	−24	30	30	48	−6	−6
3	0	648(2, 0) =	2	−34	−4	−18	−24	12	30	−24	−42	12
3	0	648(4, 0) =	2	−34	−4	18	−24	−24	−6	48	30	−24
3	0	648(5, 0) =	2	−34	−4	−18	−24	−42	−42	−24	30	30
3	0	648(7, 0) =	2	−34	−4	18	−24	−6	−24	48	−24	30
3	0	648(8, 0) =	2	−34	−4	−18	−24	30	12	−24	12	−42
3	1	648(1, 0) =	2	−34	−4	18	48	−6	30	−24	−6	−6
3	1	648(2, 0) =	2	−34	−4	−18	−24	12	−6	48	−42	12
3	1	648(4, 0) =	2	−34	−4	18	48	12	−6	−24	−6	−24
3	1	648(5, 0) =	2	−34	−4	−18	−24	−42	−6	48	30	−6
3	1	648(7, 0) =	2	−34	−4	18	48	−6	−24	−24	12	30
3	1	648(8, 0) =	2	−34	−4	−18	−24	30	12	48	12	−6
3	2	648(1, 0) =	2	−34	−4	18	−24	−6	−6	−24	30	−42
3	2	648(2, 0) =	2	−34	−4	−18	48	−24	−6	−24	30	48
3	2	648(4, 0) =	2	−34	−4	18	−24	−24	−42	−24	−6	48
3	2	648(5, 0) =	2	−34	−4	−18	48	30	−42	−24	−6	−6
3	2	648(7, 0) =	2	−34	−4	18	−24	30	48	−24	−24	−6
3	2	648(8, 0) =	2	−34	−4	−18	48	−6	48	−24	−24	−42
1	0	648(1, 0) =	2	−34	−4		−24	12	−24	12	12	12
1	0	648(2, 0) =	2	−34	17	−9	96	24	42	−66	−12	−12
1	0	648(3, 0) =	2	−34	−1	9	−30	24	−12	60	−12	42
1	0	648(4, 0) =	2	−34	−4		−24	30	48	12	30	−24
1	0	648(5, 0) =	2	−34	−1	45	−30	−12	−30	−30	−12	42
1	0	648(6, 0) =	2	−34	−1	9	−30	−12	42	6	24	−30
1	0	648(7, 0) =	2	−34	−4		−24	−42	−24	12	−42	12
1	0	648(8, 0) =	2	−34	−1	−63	−30	−12	−12	24	24	−30
1	1	648(0, 0) =	2	−70	−1	9	24	−12	6	−66	−12	−12
1	1	648(1, 0) =	2	−34	−4		12	−24	12	12	−24	−24
1	1	648(2, 0) =	2	−34	−1	45	24	−12	6	6	−12	−12
1	1	648(3, 0) =	2	−34	−1	9	6	24	−12	24	−12	6
1	1	648(4, 0) =	2	−34	−4		12	30	12	12	30	−24
1	1	648(5, 0) =	2	−34	−1	−63	−30	−12	6	6	24	6
1	1	648(6, 0) =	2	−34	−1	9	6	−12	6	−30	24	6
1	1	648(7, 0) =	2	−34	−4		12	−6	−24	12	−6	48
1	1	648(8, 0) =	2	−34	17	−9	−66	24	−12	24	−12	6
1	2	648(1, 0) =	2	−34	−4		12	12	−24	−24	12	−24
1	2	648(2, 0) =	2	−34	−1	−63	60	−12	6	−30	24	24
1	2	648(3, 0) =	2	−34	−1	9	−30	24	24	24	−12	6
1	2	648(4, 0) =	2	−34	−4		12	−6	12	−24	−6	12
1	2	648(5, 0) =	2	−34	17	−9	−30	24	−30	42	−12	6
1	2	648(6, 0) =	2	−34	−1	9	−30	−12	6	−30	24	−30
1	2	648(7, 0) =	2	−34	−4		12	−6	12	−24	−6	12
1	2	648(8, 0) =	2	−34	−1	45	6	−12	24	24	−12	−30

5. These comprise Table 6. A complete listing of all cyclotomic numbers of order 18 (f odd and f even) has been deposited in the unpublished mathematical tables file of Mathematics of Computation. The determination of L, M, c_0, $\cdots$, c_5 was discussed in Section 3.

Similarly, for f even, as 3 is always a quadratic residue of primes of the form $p = 36f' + 1$, we have $T \equiv 0, 2, 4 \pmod 6 \equiv 0, 2, 1 \pmod 3$. Hence, we arrive at the same 8 classes as before (see Table 4). Primes belonging to these classes are 8929, 397, 73, 829, 37, 2341, 109 and 433, respectively.

The calculation itself was carried out on an IBM 7094. Once the equations were determined, the cyclotomic numbers were computed for several primes and the results were checked against a direct calculation based on Eq. (1.1).

5. Applications To Difference Sets. A (v, k, λ)-difference set D is a set of k distinct residues $d_1, \cdots, d_k$ modulo v for which the congruence

$$d_i - d_j \equiv a \pmod v$$

has exactly λ solution pairs d_i, d_j for each a, $1 \leqq a \leqq v - 1$. If D is a difference set consisting of the eth power residues modulo a prime $p = v$, then D is called a *residue difference set.* If a difference set consists of the eth power residues of a prime p together with zero, then it is called a *modified residue difference set.*

Letting $p = ef + 1$, Emma Lehmer [8] showed that no residue or modified residue difference set exists if f is even. When f is odd, she gave the following necessary and sufficient conditions: For residue difference sets

$$e(i, 0)_e = (f - 1) \qquad (i = 0, 1, \cdots, \tfrac{1}{2}e - 1) \tag{5.1}$$

and for modified residue difference sets

$$e[1 + (0, 0)_e] = e(i, 0)_e = f + 1 \qquad (i = 1, 2, \cdots, \tfrac{1}{2}e - 1). \tag{5.2}$$

Hence, we can use the cyclotomic number formulas given in Tables 5 and 6 to establish

THEOREM. *The only residue difference set or modified residue difference set which exists for $e = 18$ is the trivial* 19-1-0 *difference set.*

Proof. We have only to test (5.1) and (5.2) in each of the eight possibilities provided by the classes of B, T. Sometimes both (5.1) and (5.2) can be ruled out together.

Case 1. $B \equiv 0 \pmod 9$ and $T \equiv 0 \pmod 3$. Here Table 6 shows that if $(3, 0) = (6, 0)$, as they must be to satisfy either (5.1) or (5.2), we have $M = 0$. Thus, as (see Section 3)

$$4v = L^2 + 27M^2, \qquad L \equiv 7 \pmod 9 \tag{5.3}$$

we have $4v = L^2$ which contradicts the primality of v. Hence, both types of residue difference sets are ruled out for this case.

Case 2. The four possibilities $(B, T) \equiv (0, 1), (3, 0), (3, 1)$ and $(3, 2)$ can all be eliminated in the same way. Equate the cyclotomic number $(1, 0)$ with $(4, 0)$, $(1, 0)$ with $(7, 0)$, $(2, 0)$ with $(5, 0)$, and $(2, 0)$ with $(8, 0)$. This produces four homogeneous linear equations in c_1, c_2, c_4, and c_5 for which the coefficient matrix has nonzero determinant. Thus, $c_1 = c_2 = c_4 = c_5 = 0$, which is impossible because

then $R(1, 1)_9$ is in the wrong field (see [4]). Thus, no residue difference sets and no modified residue difference sets exist for these particular index pairs (B, T).

Case 3. Ind $2 \equiv 1 \pmod 9$ and Ind $3 \equiv 0 \pmod 3$. The equality of the $(i, 0)$, $i = 1, \cdots, 8$, yields $4M = -3c_2$ and $4L = -19c_2$. Thus, $c_2 \equiv 0 \pmod 4$; let $c_2 = 4c$ then $v = 151c^2$ from (5.3). Hence v prime only if $v = 151$, but $151 \not\equiv 1 \pmod{18}$. Hence, neither type of residue difference set exists in this case.

Case 4. Ind $2 \equiv 1 \pmod 9$ and Ind $3 \equiv 1 \pmod 3$. Here the equality of the $(i, 0)$, $i = 1, \cdots, 8$, implies $c_3 = 0$ and $c_0 = -2M$. If we are to have a residue difference set, then $648(0, 0) = 2v - 38$ is the common value of $648(i, 0)$, $i = 1, \cdots, 8$. Hence, $L = 7$ and $M = -1$, so $v = 19$ and we have the trivial 19-1-0 difference set of the theorem.

If a modified residue difference set exists here, then $648[(0, 0) + 1] = 2v + 34$, which is also the common value of $648(1, 0), \cdots, 648(8, 0)$. Using $c_3 = 0$ and $c_0 = -2M$, we derive $M = 17$ and $L = 119''$ which is not congruent to 7 (mod 9). Hence, no such difference set exists.

Case 5. Ind $2 \equiv 1 \pmod 9$ and Ind $3 \equiv 2 \pmod 3$. From the equality of (1,0), $\cdots$, (8, 0) we deduce that $3c_0 = 4c_4 - 5c_5$, $c_1 = 3c_4 - 4c_5$, $c_2 = 2c_4 - 3c_5$, $c_3 = -c_2$. Now $v, c_0, \cdots, c_5$ must satisfy (see Section 3)

$$v = \left(\sum_{i=0}^{5} c_i \beta^i\right)\left(\sum_{i=0}^{5} c_i \beta^{-i}\right) \tag{5.4}$$

where β is a primitive 9th root of unity. We use the above values in (5.4) and reduce by means of $\beta^6 + \beta^3 + 1 = 0$ to find

$$v = \sum_{i=0}^{5} \alpha_i \beta^i$$

where

$$\alpha_1 = c_0c_1 + c_1c_2 + c_2c_3 + c_3c_4 + c_4c_5 - (c_0c_2 + c_1c_3 + c_2c_4 + c_3c_5).$$

Then

$$3\alpha_1 = 16c_4^2 - 48c_4c_5 + 41c_5^2 = 16(c_4 - 1.5c_5)^2 + 5c_5^2$$

which must be zero for (5.4) to be satisfied. This implies $c_4 = c_5 = 0$ and thus, $c_0 = c_1 = c_2 = c_3 = 0$ also. Hence, no difference set of either type exists for this case. Thus, we have proved the theorem.

As a further application of the cyclotomic numbers of order 18, we investigate difference sets with the parameters $v, k, \lambda = 127, 63, 31$. (This work was suggested by Professor M. Hall, Jr.) In order to do this, we must recall some of the basic results on difference sets (see [5, p. 58]). Given the difference set $D = \{d_1, \cdots, d_k\}$ then for any integer s the set $\{d_1 + s, \cdots, d_k + s\} \equiv D + s$ taken modulo v is also a difference set, called a *shift* of the set D. For any integer t, $(t, v) = 1$, the set $\{td_1, \cdots, td_k\} \equiv tD$ taken modulo v is a difference set with the same parameters v, k, λ. If $D_1 = tD_2 + s$ for some t, s, $(t, v) = 1$, then the two difference sets D_1, D_2 are called *equivalent*. If $(t, v) = 1$ and $tD = D + s$ for some s, then t is called a *multiplier* of the difference set D. If n_1 is a divisor of $n = k - \lambda$ such that $(n_1, v) = 1$, $n_1 > \lambda$, and if t is an integer such that for each prime p dividing n_1 there is an

integer j such that $p^j \equiv t \pmod{v}$, then t is a multiplier of every difference set with these particular parameters v, k, λ.

In addition to these facts we need the concept of an *index class*. If g is a primitive root of an odd prime $p = ef + 1$, the set of those i ($i = 1, 2, \cdots, p - 1$) for which $i \equiv g^{j+eb} \pmod{p}$, $b = 0, 1, \cdots, f - 1$ is called the *index class* j. (An index class depends on p, e, g as well as j, but in our application p, e and g are fixed so we do not need to complicate matters by mentioning them.)

In our case $(v, k, \lambda) = (127, 63, 31)$, so $n = 32$ and 2 is a multiplier of any such difference set by the above result. Now associated with any multiplier there is at least one shift $D + s$ fixed by the multiplier [10], which we may assume to be D. Using the multiplier 2, the residues $0, 1, 2, \cdots, 126$ can be divided into disjoint sets of numbers which are contained in the fixed shift entirely or not at all. These are: (0), $(1, 2, 2^2, 2^3, 2^4, 2^5, 2^6)$, $(3, 2\cdot 3, 2^2\cdot 3, \cdots, 2^6\cdot 3)$, $\cdots$, $(i, 2i, 2^2 i, \cdots, 2^6 i)$, $\cdots$ with a total of 19 sets. Since 3 is a primitive root of 127 and $3^{72} \equiv 2 \pmod{127}$, the eighteen seven-member sets $(i, 2i, \cdots, 2^6 i)$ coincide with the index classes for $p = 127$, $e = 18$. Hence, the 18 seven-member sets can be represented by their index class numbers $j = 0, 1, \cdots, 17$.

Since 2 was a multiplier, we see that every 127, 63, 31 difference set is composed of exactly nine of these index classes. A computer search was performed selecting nine of these eighteen classes in all possible ways and checking which were difference sets. Rejecting equivalent difference sets, we found exactly six solutions, which in terms of the index class numbers are:

0, 2, 4, 6, 8, 10, 12, 14, 16	quadratic residues [12, p. 133],
0, 1, 3, 6, 7, 9, 12, 13, 15	Hall's set $4x^2 + 27$ (Theorem 2.2, [6]),
0, 1, 2, 3, 5, 6, 7, 10, 16	linear recurrence set [5, pp. 52, 59],
0, 1, 2, 3, 4, 6, 7, 10, 12	new,
0, 1, 2, 3, 5, 11, 12, 15, 16	new,
0, 1, 3, 5, 8, 9, 12, 14, 15	new.

Following Hall (Theorem 2.2, [6]) we shall use cyclotomic numbers to see if any new families of difference sets arise here. We need only investigate the last four cases, since the first two are in families which are *based on cyclotomy*. The third one is a member of the known infinite family indicated above, but since that family is *not* based on cyclotomy, one might ask whether it could also be a member of a new family which is related to the cyclotomic numbers of order 18. Unfortunately, no new cyclotomic family of difference sets arises here. Thus, from the point of view of this paper, the last four difference sets above represent nothing more than peculiarities of the prime 127.

Eq. (1.1) shows us that the cyclotomic number (k, h) is the number of solutions of

$$\alpha - \beta \equiv 1 \pmod{v}$$

with α in index class k and β in index class h. Multiplying (1.1) through by d in index class s we have

$$g^{ex+k+s} - g^{ey+h+s} \equiv d \pmod{v}.$$

Thus, for fixed d in class s, the congruence

$$\alpha - \beta \equiv d \pmod{v} \tag{5.6}$$

has exactly $(k - s, h - s)$ solutions with α in class k and β in class h. Hence, the number

$$N_s = \sum_{i=1}^{9} \sum_{j=1}^{9} (z_i - s, z_j - s)$$

is the number of solutions of (5.6) for fixed d in class s when the difference set is composed of index classes $z_1, \cdots, z_9$. So if a difference set exists, $N_0 = \cdots = N_{17} = \lambda$. Now $v = 127$ belongs to the case $e = 18, f$ odd, for Ind $2 \equiv 0 \pmod 9$ and Ind $\equiv 1 \pmod 3$. For odd f, Eq. (2.2) yields $N_i = N_{9+i}$ $(i = 0, \cdots, 8)$; thus it is sufficient to consider $N_0, \cdots, N_8$ alone. Consulting Table 5 we see that if the linear recurring set is to generalize we want a family of solutions to $N_0 = \cdots = N_8 = \lambda$, with

$$648N_0 = 162v - 24L - 24c_0 + 138c_1 - 96c_2 + 192c_3 - 186c_4 + 138c_5 - 486,$$

$$648N_1 = 162v - 18M - 144c_0 + 18c_1 - 198c_2 - 72c_3 - 72c_4 - 810,$$

$$648N_2 = 162v + 18L + 72M + 108c_0 - 72c_1 + 144c_2 + 90c_3 - 144c_5 - 486,$$

$$648N_3 = 162v + 12L - 108M + 120c_0 - 96c_1 - 6c_2 - 96c_3 + 66c_4 - 42c_5 - 486,$$

$$648N_4 = 162v - 18M + 288c_0 - 72c_1 - 18c_2 - 72c_3 + 126c_4 + 162c_5 - 162,$$

$$648N_5 = 162v - 18L + 72M - 36c_0 + 288c_1 + 72c_2 - 54c_3 - 144c_4 - 144c_5 - 486,$$

$$648N_6 = 162v + 12L + 108M - 96c_0 - 144c_1 + 246c_2 - 96c_3 + 264c_4 + 48c_5 - 486,$$

$$648N_7 = 162v - 18M - 144c_0 - 18c_1 - 72c_2 + 144c_3 - 126c_4 - 18c_5 - 810,$$

$$648N_8 = 162v - 90M - 72c_0 - 72c_1 - 72c_2 - 36c_3 + 72c_4 - 162.$$

These equations have only the solution associated with $v = 127$.

Similarly for the remaining three difference sets above we used Table 5 to express $N_0, \cdots, N_8$ in terms of $v, L, M, c_0, \cdots, c_5$. We found in each of these cases only one solution $(v = 127)$.

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

1. H. Davenport & H. Hasse, "Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen," *J. Reine Angew. Math.*, v. 172, 1934, pp. 151–182.
2. L. E. Dickson, "Cyclotomy, higher congruences and Waring's problem," *Amer. J. Math.*, v. 57, 1935, pp. 391–424, 463–474.
3. L. E. Dickson, "Cyclotomy and trinomial congruences," *Trans. Amer. Math. Soc.*, v. 37, 1935, pp. 363–380.
4. L. E. Dickson, "Cyclotomy when e is composite," *Trans. Amer. Math. Soc.*, v. 38, 1935, pp. 187–200.
5. S. W. Golomb, et al., *Digital Communications with Space Applications*, Prentice-Hall, Englewood Cliffs, N. J., 1964.
6. M. Hall, Jr., "A survey of difference sets," *Proc. Amer. Math. Soc.*, v. 7, 1956, pp. 975–986. MR **18**, 560.
7. M. Kraitchik, *Recherches sur la Théorie des Nombres*, Vol. 1, Paris, 1924.

8. E. LEHMER, "On residue difference sets," *Canad. J. Math.*, v. 5, 1953, pp. 425–432. MR **15,** 10.

9. E. LEHMER, "On the number of solutions of $u^k + D \equiv w^2 \pmod{p}$, " *Pacific J. Math.*, v. 5, 1955, pp. 103–118. MR **16,** 798.

10. R. L. MCFARLAND & H. B. MANN, "On multipliers of difference sets," *Canad. J. Math.*, v. 17, 1965, pp. 541–542. MR **31** #3347.

11. J. B. MUSKAT, "The cyclotomic numbers of order fourteen," *Acta Arith.*, v. 11, 1966, pp. 263–279.

12. H. J. RYSER, *Combinatorial Mathematics*, Carus Math. Monos., No. 14, Math. Assoc. of Amer., distributed by Wiley, New York, 1963. MR **27** #51.

13. A. L. WHITEMAN, "The cyclotomic numbers of order ten," *Proc. Sympos. Appl. Math.*, Vol. 10, pp. 95–111, Amer. Math. Soc., Providence, R. I., 1960. MR **22** #4682.

14. A. L. WHITEMAN, "The cyclotomic numbers of order twelve," *Acta Arith.*, v. 6, 1960, pp. 53–76. MR **22** #9480.

15. A. L. WHITEMAN, "The cyclotomic numbers of order sixteen," *Trans. Amer. Math. Soc.*, v. 86, 1957, pp. 401–413. MR **19,** 1160.