DIFFERENCE SETS IN ELEMENTARY ABELIAN GROUPS[1]

BY
H. B. MANN

Introduction

A difference set (v, k, λ) in a group G of order v is a set $g_1, \cdots, g_k$ of k distinct elements of G such that the equation

$$g_i g_j^{-1} = g$$

has exactly λ solutions for every $g \in G$, $g \neq 1$. A simple count gives

$$\lambda(v - 1) = k(k - 1). \tag{1}$$

Trivially G itself is a difference set with $v = k = \lambda$. Also $G - g$ for any $g \in G$ is a difference set with $k = v - 1$, $\lambda = v - 2$. These two trivial cases will be excluded in the following. The complement of a difference set is a difference set so that we may also assume

$$k < v/2, \qquad \lambda < n = k - \lambda. \tag{2}$$

A large part of the effort devoted to research on difference sets has been directed towards difference sets in cyclic groups [3] and all v, k, λ, with $k \leq 50$ for which cyclic solutions exist are now known [3], [6], [9], [10].

The present paper investigates difference sets in elementary Abelian groups of order p^m, $m > 1$. For $p = 2$ nontrivial difference sets with $k \leq v/2$ exist only for $v = 2^{2m}$, $k = 2^{2m-1} - 2^{m-1}$, $\lambda = 2^{2m-2} - 2^{m-1}$. For odd values of p the quadratic residues of $GF(p^n)$ form a difference set if and only if $p^n \equiv 3\ (4)$. A new necessary condition for the existence of difference sets in elementary p groups is derived. An enumeration of all parameter combinations with $v = p^m \leq 2500$, $m > 1$ leaves only nine cases undecided.

1. Elementary 2-groups

For $v = 2^{2m}$, $k = 2^{2m-1} - 2^{m-1}$, $\lambda = 2^{2m-2} - 2^{m-1}$ difference sets (v, k, λ) have been constructed by P. K. Menon [7]. According to R. J. Turyn [10] a solution for this set of parameters can easily be obtained as follows: Represent the direct product of m four-groups by points $(g_1, \cdots, g_m)$, where

$$(g_1, \cdots, g_m)(g_1', \cdots, g_m') = (g_1 g_1', \cdots, g_m g_m').$$

Let D be the set of points containing an odd number of ones. Then D is a difference set with parameters $k = 2^{2m-1} - 2^{m-1}$, $\lambda = 2^{2m-2} - 2^{m-1}$.

We shall show that these are the only values of n for which nontrivial 2^m, k, λ configurations exist.

Received November 7, 1963.

[1] Sponsored by the Mathematics Research Center, U. S. Army, Madison, Wisconsin.

THEOREM 1. *If there exists a nontrivial* $2^m, k, \lambda$ *configuration* then $k - \lambda = n = 2^{2s}$, $v = 2^{2s+2}$.

We may assume $k < v/2$. Since v is even, n must be a square. (See e.g. [6].) Put $n = 2^{2s}n_1^2$, $n_1 \equiv 1\ (2)$. From (1) we then have

$$\lambda 2^m = k^2 - 2^{2s}n_1^2$$

and since $n < v$ we must have

$$k = 2^s k_1\,, \qquad \lambda = 2^s(k_1 - 2^s n_1^2) = 2^s\lambda_1$$

where $k_1 \equiv 1\ (2)$. We get

$$\lambda_1 2^{m-s} = (k_1 - n_1)(k_1 + n_1).$$

Either $k_1 - n_1$ or $k_1 + n_1$ must be divisible by 2^{m-s-1} and since $k_1 < 2^{m-s-1}$ we must have $k_1 + n_1 \equiv 0\ (2^{m-s-1})$. But $k_1 + n_1 < 2^{m-s}$ hence

$$k_1 + n_1 = 2^{m-s-1}, \qquad k_1 - n_1 = 2\lambda_1\,, \qquad k_1 - 2^s n_1^2 = \lambda_1\,.$$

Solving these equations leads to

$$2^{2s}n_1^2 = n = 2^{m-2}$$

and since n is a square m must be even. This completes the proof of Theorem 1.

2. Elementary p-groups with p odd

The theorems on difference sets in the field of residues mod p, p a prime, given by S. Chowla [1] and by Emma Lehmer [5] and the underlying theory of L. E. Dickson carry over without change to any finite field. This yields

THEOREM 2. *The quadratic residues of a finite field of order* p^m *form a difference set if and only if* $p^m \equiv 3\ (4)$.

To give a self contained proof of Theorem 2 denote by ρ generically a quadratic residue, by ν a nonresidue in $GF(p^m)$, $p^m \equiv 3\ (4)$. Since -1 is a ν we may write

$$\rho_1 - \rho_2 = \rho + \nu.$$

Now if $\rho + \nu = a \neq 0$ then $ba^{-1}\rho + ba^{-1}\nu = \rho_1 + \nu_1 = b$. Hence every element of $GF(p^n)$ has the same number of representations in the form $\rho_1 - \rho_2$, Q.E.D.

Theorem 2 is very useful. Difference sets (v, k, λ) can often be obtained in p-groups which do not exist in cyclic groups. An example is $v = 27$, $k = 13$, $\lambda = 6$. The difference sets obtained in this way also supply Hadamard matrices with comparatively simple properties.

The other theorems of S. Chowla and E. Lehmer also carry over to all finite fields. The theorems on higher residue difference sets applied to finite fields of order p^m, $m \geq 2$ are however useful only as nonexistence theorems

since the necessary and sufficient arithmetical conditions are not likely ever to be satisfied for $m \geq 2$. We also have: If $p^m - 1 = ef$ and $f \equiv 0\ (2)$ then the e^{th} residues do not form a difference set. This theorem, proved by Emma Lehmer [5], also follows from Theorem 5 of [6].

Computation yields 72 solutions of (1) with $v = p^m \leq 2500$, $m > 1$. For five of these parameter values residue difference sets exist. For 51 values difference sets are impossible by the theorems in [6]. Seven more are impossible by the theorems of Section 3 of this paper. This leaves 9 cases undecided. These are

v	k	λ	n
3^4	16	3	13
11^2	40	13	27
19^2	136	51	85
29^2	120	17	103
31^2	256	68	188
11^3	210	33	177
11^3	266	53	213
13^3	793	286	507
3^6	273	102	171

It is worth noting that there exists a cyclic difference set with parameters 11^2, 40, 13.

The table at the end of this paper enumerates all solutions of (1) with $2500 \geq v = p^m$, $m > 1$, p a prime. If a difference set is known not to exist for the p group of order v we give in the last column either the relation which proves the non-existence by Theorem 3 of [6] or the theorems of the next section of this paper which show nonexistence.

3. A necessary condition for existence of a difference set (v, k, λ) in an elementary p-group

THEOREM 3. *If the quadratic residues* mod p *are multipliers of the elementary Abelian difference set D with parameters p^m, k, λ then the equation*

$$x^2 + py^2 = 4n \tag{3}$$

is solvable. Let $(x_1, y_1), (x_2, y_2), \cdots, (x_l, y_l)$ be the solutions of (3) satisfying the additional conditions

(i) $2k \equiv x\ (p)$, (ii) $k + \frac{1}{2}(p-1)x \geq 0$, (iii) $k \geq \frac{1}{2}(x + |y|p)$.

Then $l > 0$ and either the system

$$\begin{aligned} k + \tfrac{1}{2}(p-1)(x_1z_1 + \cdots + x_lz_l) &= 0 \\ z_1 + \cdots + z_l &= (p^m - 1)/)p - 1) \end{aligned} \tag{4a}$$

or the system

$$k + \tfrac{1}{2}(p-1)(x_1 z_1 + \cdots + x_l z_l) = p^m$$
$$z_1 + \cdots + z_l = (p^m - 1)/(p-1) \tag{4b}$$

has a solution in nonnegative integers $z_1, \cdots, z_l$.

We first prove

PROPOSITION 1. $n \neq p^t$, $t > 0$.

Proof. From

$$\lambda p^m = k^2 - n = k^2 - p^t, \qquad m > t$$

we get $t = 2t_1$, $k = \mu p^{t_1}$, $\lambda = p^{t_1}(\mu - p^{t_1})$. Hence

$$(\mu - p^{t_1})p^{m-t_1} = (\mu - 1)(\mu + 1).$$

Since $(\mu - 1, \mu + 1) = 1$ or 2 we get

$$p^{m-t_1} \leq \mu + 1,$$
$$k \geq p^m - p^{t_1} > p^m - p^{m/2} > p^m/2 = v/2$$

contradicting (2).

COROLLARY TO PROPOSITION 1. *The number* (-1) *cannot be a multiplier.*

This follows from Proposition 1 and from [6, Corollary 5.2].

We proceed to prove Theorem 3. From the corollary to Proposition 1 it follows that $p \equiv 3\ (4)$. Let t generate the quadratic residues mod p. Then $(t-1) \not\equiv 0\ (p)$ and there exists a difference set D fixed under all quadratic residues. It follows that all characters $\chi(D)$ (for the notation used here see [6]) are fixed under the isomorphism $\rho \to \rho^t$ of the field $R(\rho)$, where ρ is a primitive p^{th} root of unity and R the field of rational numbers. Hence $\chi(D) \in R(\sqrt{-p})$,

$$\chi(D) = (x + y\sqrt{-p})/2$$

where x, y are rational integers. Hence

$$4n = 4\chi(D)\overline{\chi(D)} = x^2 + py^2.$$

Let a_i elements of D have the character ρ^i under χ. Then for a suitably chosen value of $\sqrt{-p}$ we have

$$\sum a_i = k,$$
$$\sum a_i \rho^{si} = (x + y(\tfrac{s}{p})\sqrt{-p})/2, \qquad s = 1, 2, \cdots, p-1, \tag{5}$$

where $(\frac{s}{p})$ is the Legendre symbol. (The automorphism $\rho \to \rho^s$ carries $\sqrt{-p}$ into $(\frac{s}{p})\sqrt{-p}$.)

Summing the equations (5) gives

$$pa_0 = k + \tfrac{1}{2}(p-1)x.$$

Whence

$$2k \equiv x\ (p), \qquad k + \tfrac{1}{2}(p-1)x \geq 0.$$

Multiplying the s^{th} equation of (5) by ρ^{-si} and summing yields

$$pa_i = k - \tfrac{1}{2}x + \tfrac{1}{2}y\sqrt{-p}\,\textstyle\sum_1^{p-1}\left(\frac{s}{p}\right)\rho^{-is}.$$

By a well known formula [4] we have

$$\textstyle\sum_s \left(\frac{s}{p}\right)\rho^{-is} = \pm\left(\frac{i}{p}\right)\sqrt{-p}, \qquad i = 1, \cdots, p-1$$

so that

$$pa_i = k - \tfrac{1}{2}x \mp \left(\frac{i}{p}\right)\tfrac{1}{2}yp$$

which shows that at least one of the solutions of (3) satisfies the additional conditions (i), (ii) and (iii).

Let $x_1, \cdots, x_l$ be the values of x satisfying equation (3) and conditions (i), (ii) and (iii) and suppose that for Z_i characters χ we have

$$\chi(D) = (x_i + y_i\sqrt{-p})/2.$$

If χ is such a character then summing over all $p-1$ conjugate characters gives $(\frac{1}{2}(p-1)x_i$. Moreover $Z_i \equiv 0\,(\frac{1}{2}(p-1))$, $Z_i = \frac{1}{2}(p-1)z_i$. The sum of all characters divided by p^m gives the coefficient of the unit element in D which is either 1 or 0 and this gives either (4a) or (4b) which completes the proof of Theorem 3.

COROLLARY 1. *If under the conditions of Theorem* 3 *the equation* $x^2 + py^2 = 4n$ *and the conditions* (i), (ii), (iii) *have only one solution then*

$$k = (p^m - 1)/2, \qquad m \equiv 1\ (2).$$

Proof. We get from (4a) and (2)

$$k + \tfrac{1}{2}(p^m - 1)x = 0, \qquad k = \tfrac{1}{2}(p^m - 1), \tag{6a}$$

or

$$k + \tfrac{1}{2}(p^m - 1)x = 1, \qquad k = \tfrac{1}{2}(p^m + 1). \tag{6b}$$

But (6b) does not satisfy (2). Furthermore $\lambda = (p^m - 3)/4$ hence $m \equiv 1\ (2)$.

COROLLARY 2. *If* $p > 3$ *and the conditions of Theorem* 3 *hold then* n *is not a prime.*

Otherwise there are only at most two factorizations $n = \alpha\bar{\alpha} = (-\alpha)(-\bar{\alpha})$ in $R(\sqrt{-p})$. Hence equation (3) has only one solution. We then have $n = (p^m + 1)/4$, $m \equiv 1\ (2)$ and so n has the factor $(p+1)/4$.

THEOREM 4. *If* $p = 2q + 1$, q *a prime and if no prime divisor of* n *is congruent to* 1 mod p *then the quadratic residues* mod p *are multipliers of any elementary Abelian difference set* (p^m, k, λ) *and* n *is not a prime.*

TABLE 1

Solutions of equation 1 for $v = p^m \leq 2500, \quad m > 1$

v	k	λ	n	Disposition
5^2	9	3	6	$2^2 \equiv -1\ (5)$
7^2	16	5	11	Theorem 4
11^2	16	2	14	$\left(\frac{2}{11}\right) = -1$
11^2	25	5	20	$\left(\frac{2}{11}\right) = -1$
11^2	40	13	27	undecided
13^2	49	14	35	$\left(\frac{5}{13}\right) = -1$
13^2	57	19	38	$\left(\frac{2}{13}\right) = -1$
13^2	64	24	40	$\left(\frac{2}{13}\right) = -1$
17^2	64	14	50	$2^4 \equiv -1\ (17)$
19^2	81	18	63	$\left(\frac{3}{19}\right) = -1$
19^2	136	51	85	undecided
19^2	145	58	87	$\left(\frac{3}{19}\right) = -1$
23^2	33	2	31	Theorem 4
23^2	144	39	105	$\left(\frac{5}{23}\right) = -1$
23^2	177	59	118	Theorem 3
29^2	105	13	92	$\left(\frac{2}{29}\right) = -1$
29^2	120	17	103	undecided
29^2	225	60	165	$\left(\frac{3}{29}\right) = -1$
29^2	280	93	187	$\left(\frac{11}{29}\right) = -1$
29^2	336	134	202	$\left(\frac{2}{29}\right) = -1$
29^2	385	176	209	$\left(\frac{11}{29}\right) = -1$
29^2	400	190	210	$\left(\frac{3}{29}\right) = -1$
31^2	256	68	188	undecided
31^2	321	107	214	Corollary 3.1
31^2	385	154	231	$\left(\frac{3}{31}\right) = -1$
37^2	153	17	136	$\left(\frac{2}{37}\right) = -1$
37^2	361	95	266	$\left(\frac{2}{37}\right) = -1$
37^2	513	192	323	$3^9 \equiv -1\ (37)$
41^2	225	30	195	$\left(\frac{3}{41}\right) = -1$
41^2	336	67	269	$(269)^5 \equiv -1\ (41)$
41^2	385	88	297	$\left(\frac{3}{41}\right) = -1$
41^2	400	95	305	$5^{10} \equiv -1\ (41)$
41^2	561	187	374	$2^{10} \equiv -1\ (41)$
41^2	721	309	412	$2^{10} \equiv -1\ (41)$
41^2	736	322	414	$2^{10} \equiv -1\ (41)$
43^2	232	29	203	$\left(\frac{7}{43}\right) = -1$
43^2	385	80	305	$\left(\frac{5}{43}\right) = -1$
43^2	441	105	336	$\left(\frac{2}{43}\right) = -1$
43^2	561	170	391	$\left(\frac{17}{43}\right) = -1$
43^2	616	205	411	$\left(\frac{3}{43}\right) = -1$
43^2	672	244	428	$\left(\frac{2}{43}\right) = -1$

TABLE 1 (*continued*)

v	k	λ	n	Disposition
43^2	792	339	453	$\left(\frac{3}{43}\right) = -1$
47^2	576	150	426	Corollary 3.1, Theorem 4
47^2	736	245	491	Theorem 4
47^2	897	364	533	$\left(\frac{13}{47}\right) = -1$
3^3	13	6	7	exists (Theorem 2)
5^3	32	8	24	$\left(\frac{3}{5}\right) = -1$
7^3	19	1	18	$\left(\frac{3}{7}\right) = -1$
7^3	153	68	85	$\left(\frac{5}{7}\right) = -1$
7^3	171	85	86	exists (Theorem 2)
11^3	190	27	163	Theorem 4
11^3	210	33	177	undecided
11^3	266	53	213	undecided
11^3	400	120	280	$\left(\frac{2}{11}\right) = -1$
11^3	456	156	300	$\left(\frac{2}{11}\right) = -1$
11^3	476	170	406	$\left(\frac{2}{11}\right) = -1$
11^3	665	332	333	exists (Theorem 2)
13^3	244	27	217	$\left(\frac{7}{13}\right) = -1$
13^3	549	137	412	$\left(\frac{2}{13}\right) = -1$
13^3	793	286	507	undecided
3^4	16	3	13	undecided
5^4	144	33	111	$\left(\frac{3}{5}\right) = -1$
5^4	208	69	139	$139 \equiv -1\ (5)$
5^4	273	119	154	$\left(\frac{3}{5}\right) = -1$
7^4	225	21	204	$\left(\frac{3}{7}\right) = -1$
7^4	576	138	438	$\left(\frac{3}{7}\right) = -1$
7^4	801	267	534	$\left(\frac{3}{7}\right) = -1$
3^5	121	60	61	exists (Theorem 2)
3^6	105	15	90	$2 \equiv -1\ (3)$
3^6	169	39	130	$2 \equiv -1\ (3)$
3^6	273	102	171	undecided
3^7	1093	546	547	exists (Theorem 2)

If $p = 2q + 1$ then all divisors of n are quadratic residues [6, Theorem 3] and must have order q. Let $q_1, \cdots, q_s$ be primes and

$$n = q_1^{l_1} \cdots q_s^{l_s}.$$

Then

$$q_i^{f_i} \equiv q_s\ (p).$$

Hence q_s is multiplier [5, Corollary 4.1]. Hence every q_i is multiplier. By Corollary 2 it follows that n is not a prime.

In applying Theorem 3 to 31^2, 321,107 one has to apply a result of Morris Newman [8] according to which a prime p is multiplier if $2p = n > \lambda$. New-

man announced this result only for cyclic difference sets but his proof can be modified to apply to any Abelian difference set.

References

1. S. Chowla, *A property of biquadratic residues*, Proc. Nat. Acad. Sci. India. Part A, vol. 14 (1944), pp. 45–46.
2. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math., vol. 57, (1935), pp. 391–424.
3. Marshall Hall Jr., *A survey of difference sets*, Proc. Amer. Math. Soc., vol. 7 (1956), pp. 975–986.
4. E. Hecke, *Vorlesungen ueber die Theorie der algebraischen Zahlen*, 2. Auflage, Leipzig, Geest and Portig, 1954, § 58.
5. Emma Lehmer, *On residue difference sets*, Canad. J. Math., vol. 5 (1953), pp. 425–432.
6. H. B. Mann, *Balanced incomplete block designs and Abelian difference sets*, Illinois J. Math., vol. 8 (1964), pp. 252–261.
7. P. K. Menon, *Difference sets in Abelian groups*, Proc. Amer. Math. Soc., vol. 11 (1960), pp. 368–377.
8. Morris Newman, *Multipliers of difference sets*, Canad. J. Math., vol. XV (1963), pp. 121–124.
9. R. A. Rankin, *Difference sets*, Acta Arith., vol. 9 (1964), pp. 161–168.
10. R. J. Turyn, *Character sums and difference sets*, Thesis, Harvard University, Cambridge, Massachusetts.

Ohio State University
Columbus, Ohio