[4] — *Algebraic functions and an analogue of the geometry of numbers: the Riemann–Roch theorem*, Archiv der Mathematik, 17 (1967), pp. 383–393.
[5] C. Chevalley, *Algebraic functions of one variable*, American Math. Soc. Surveys No. 6, New York 1951.
[6] H. Davenport, *Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields*, Quart. J. of Math. (Oxford) (2) 1 (1950), pp. 54–62.
[7] — *Euclid's algorithm in cubic fields of negative discriminant*, Acta Mathematica 84 (1950), pp. 159–179.
[8] — *Euclid's algorithm in certain quartic fields*, Trans. Amer. Math. Soc. 68 (1950), pp. 508–532.

KING'S COLLEGE LONDON
London, England

Received on 25. 3. 1970

ACTA ARITHMETICA
XVIII (1971)

Cyclotomy and complementary difference sets

by

G. Szekeres (Kensington, New South Wales)

In memory of H. Davenport

1. Let $(\boldsymbol{G}, +)$ be an additive abelian group of order n, $\boldsymbol{A}, \boldsymbol{B}, \ldots, \boldsymbol{C}$ k non-empty subsets of $\boldsymbol{G}$, each containing m elements. The sets $\boldsymbol{A}, \boldsymbol{B}, \ldots, \boldsymbol{C}$ are said to form a *k-ary difference system* in $\boldsymbol{G}$ if for each non-zero $\delta \in \boldsymbol{G}$ the total number of solutions of the k equations

$$\begin{aligned} \delta &= \alpha_1 - \alpha_2, \quad && \alpha_1, \alpha_2 \in \boldsymbol{A}, \\ \delta &= \beta_1 - \beta_2, && \beta_1, \beta_2 \in \boldsymbol{B}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots && \\ \delta &= \gamma_1 - \gamma_2, && \gamma_1, \gamma_2 \in \boldsymbol{C} \end{aligned} \tag{1}$$

is the same number N, independent of δ. Clearly we must have

$$(n-1)N = km(m-1). \tag{2}$$

For instance, if $\boldsymbol{G}$ is the group of residues mod 5 then $\boldsymbol{A} = \{0, 1\}$, $\boldsymbol{B} = \{0, 2\}$ is a binary difference system, with $N = 1$. The number of solutions of the individual equations (1) is of no interest, only the total number of solutions of all k equations. Ordinary difference sets correspond to the case $k = 1$.

Of particular interest are binary difference sets $\boldsymbol{A}, \boldsymbol{B}$ in a group $\boldsymbol{G}$ of order $n = 2m+1$; in this case we say that $\boldsymbol{A}, \boldsymbol{B}$ are *complementary difference sets*, provided that at least one of the sets, say $\boldsymbol{A}$, has the property that

$$a \in \boldsymbol{A} \Rightarrow -a \notin \boldsymbol{A}. \tag{3}$$

The number of solutions of (1) in a complementary difference system is $N = m-1$. Interest in complementary difference sets stems from the fact that if they exist in some $\boldsymbol{G}$ of order $2m+1$, then there also exists a skew Hadamard matrix of order $4(m+1)$ (see [5], Theorem 2).

If there exists in G an ordinary difference set A of order m with property (3), then there is also a pair of complementary difference sets, namely A and $B = A$. For instance if m is odd and $n = q$ is a prime power $\equiv 3 \pmod 4$ then we may take for G the additive group of the finite field $\mathrm{GF}(q)$ and for A and B the set of non-zero quadratic elements in $\mathrm{GF}(q)$ ([4], p. 30, Theorem 3). Similarly, if $m \equiv 2 \pmod 4$ and $n = p^{2r+1}$ is an odd power of a prime $p \equiv 5 \pmod 8$, then

$$A = C_0 \cup C_1, \quad B = C_0 \cup C_3$$

are complementary difference sets in G where G is the additive group of $\mathrm{GF}(p^{2r+1})$, C_0 is the set of non-zero fourth powers in $\mathrm{GF}(p^{2r+1})$, and $C_i = \varrho^i C_0$, $i = 1, 2, 3$, where ϱ is a generator of the multiplicative group G^* of $\mathrm{GF}(p^{2r+1})$ ([5], Theorem 5).

The purpose of this note is to extend the result to even powers of p. More specifically we shall prove:

THEOREM 1. *Let p be a prime, $p \equiv 5 \pmod 8$, $q = p^{2r}$, $r > 0$, G the additive group of $\mathrm{GF}(q)$, C_0 the set of octic residues of $\mathrm{GF}(q)$,*

$$C_i = \varrho^i C_0, \quad i = 1, 2, \ldots, 7,$$

where ϱ is a generator of the multiplicative group G^* of $\mathrm{GF}(q)$. Then

$$A = C_0 \cup C_1 \cup C_2 \cup C_3, \quad B = C_0 \cup C_1 \cup C_6 \cup C_7$$

are complementary difference sets in G.

As an immediate corollary we obtain from [5], Theorem 2:

THEOREM 2. *Let p be a prime, $p \equiv 5 \pmod 8$. Then there exists a skew Hadamard matrix of order $2(p^r+1)$ for all $r > 0$.*

The special case $q = 25$ of Theorem 1 was found earlier on a computer by D. Blatt and the author ([1]). The present note uses the method of cyclotomy, as worked out originally by Emma Lehmer ([2], [3]) for ordinary difference sets. The author is greatly indebted to D. H. and Emma Lehmer as well as to John Selfridge for helpful discussions.

2. We shall mostly adhere to Storer's definitions and notations in [4]. Let $q = 16k+9$ be a prime power $\equiv 9 \pmod{16}$, ϱ a generator of the multiplicative group G^* of $\mathrm{GF}(q)$,

$$C_i = \{\varrho^{8j+i};\ j = 0, 1, \ldots, 2k\}, \quad i = 0, 1, \ldots, 7.$$

The cyclotomic number (i, j) is defined as the number of solutions of the equation

$$\gamma_i + 1 = \gamma_j, \quad \gamma_i \in C_i, \quad \gamma_j \in C_j. \tag{4}$$

These numbers are determined as follows: First we have ([4], p. 25, Lemma 2)

$$\begin{aligned}
A &= (0,0) = (4,0) = (4,4),\\
B &= (0,1) = (3,7) = (5,4),\\
C &= (0,2) = (2,6) = (6,4),\\
D &= (0,3) = (1,5) = (7,4),\\
E &= (0,4),\\
F &= (0,5) = (7,3) = (1,4),\\
G &= (0,6) = (6,2) = (2,4),\\
H &= (0,7) = (5,1) = (3,4),\\
I &= (1,0) = (3,3) = (4,1) = (4,5) = (5,0) = (7,7),\\
J &= (1,1) = (3,0) = (4,7) = (4,3) = (5,5) = (7,0),\\
K &= (1,2) = (2,7) = (3,6) = (5,3) = (6,5) = (7,1),\\
L &= (1,3) = (1,6) = (2,5) = (6,3) = (7,5) = (7,2),\\
M &= (1,7) = (2,3) = (3,5) = (5,2) = (6,1) = (7,6),\\
N &= (2,0) = (2,2) = (4,6) = (4,2) = (6,0) = (6,6),\\
O &= (3,1) = (2,1) = (5,7) = (3,2) = (6,7) = (5,6),
\end{aligned}$$

and the numbers $A, B, \ldots, O$ are given ([4], p. 79, Lemma 30) by the following expressions:

		or	
$64A$	$= q-15-2x$		$q-15-10x-8a,$
$64B$	$= q+1+2x-4a+16y$		$q+1+2x-4a-16b,$
$64C$	$= q+1+6x+8a-16y$		$q+1-2x+16y,$
$64D$	$= q+1+2x-4a-16y$		$q+1+2x-4a-16b,$
$64E$	$= q+1-18x$		$q+1+6x+24a,$
$64F$	$= q+1+2x-4a+16y$		$q+1+2x-4a+16b,$
$64G$	$= q+1+6x+8a+16y$		$q+1-2x-16y,$
$64H$	$= q+1+2x-4a-16y$		$q+1+2x-4a+16b,$
$64I$	$= q-7+2x+4a$		$q-7+2x+4a+16y,$
$64J$	$= q-7+2x+4a$		$q-7+2x+4a-16y,$
$64K$	$= q+1-6x+4a+16b$		$q+1+2x-4a,$
$64L$	$= q+1+2x-4a$		$q+1-6x+4a,$
$64M$	$= q+1-6x+4a-16b$		$q+1+2x-4a,$
$64N$	$= q-7-2x-8a$		$q-7+6x,$
$64O$	$= q+1+2x-4a$		$q+1-6x+4a.$

The first column gives the expression when 2 is a fourth power in G, the second column, when 2 is not a fourth power in G. The numbers x, y are determined from

$$q = x^2+4y^2, \quad x \equiv 1 \pmod 4, \quad (q, x) = 1$$

if q has the form

$$q = p^{2r},\ p \equiv 5 \pmod 8 \quad \text{or} \quad q = p^{2r+1},\ p \equiv 9 \pmod{16},$$

and from

$$x = \pm p^r, \quad x \equiv 1 \pmod 4, \quad y = 0$$

if q has the form

$$q = p^{2r}, \quad p \equiv 3 \pmod 8;$$

the numbers a, b are determined from

$$q = a^2 + 2b^2, \quad a \equiv 1 \pmod 4, \quad (a, q) = 1$$

if

$$q = p^{2r},\ p \equiv 3 \pmod 8 \quad \text{or} \quad q = p^{2r+1},\ p \equiv 9 \pmod{16},$$

and from

$$a = \pm p^r, \quad a \equiv 1 \pmod 4, \quad b = 0,$$

if

$$q = p^{2r}, \quad p \equiv 5 \pmod 8.$$

We make use of the following Lemma, proved in [1], Theorem 3:

LEMMA. *With the previous notations, let*

$$\boldsymbol{A} = \boldsymbol{C}_0 \cup \boldsymbol{C}_1 \cup \boldsymbol{C}_2 \cup \boldsymbol{C}_3, \quad \boldsymbol{B} = \boldsymbol{C}_0 \cup \boldsymbol{C}_1 \cup \boldsymbol{C}_6 \cup \boldsymbol{C}_7.$$

Suppose further that the total number of solutions of the equations

$$1 = a_1 - a_2, \quad a_1, a_2 \in \boldsymbol{A}, \tag{5}$$

$$1 = \beta_1 - \beta_2, \quad \beta_1, \beta_2 \in \boldsymbol{B}$$

is $8k+3 = \frac{1}{2}(q-3)$. *Then* $\boldsymbol{A}, \boldsymbol{B}$ *are complementary difference sets in* $\boldsymbol{G}$.

In other words, if the element 1 is represented the correct number of times, then all other non-zero elements δ are represented the same number of times. Condition (3) is trivially fulfilled since $-1 \in C_4$ and $-\boldsymbol{C}_i = \boldsymbol{C}_{i+4}$ where the convention $\boldsymbol{C}_{i+8} = \boldsymbol{C}_i$ is used.

Now the number of solutions of (5) is, by (4),

$$\sum_{i=0}^{3}\sum_{j=0}^{3}(i,j) + \sum_{i=-2}^{1}\sum_{j=-2}^{1}(i,j)$$
$$= 2A+2B+C+D+G+H+4I+4J+2K+2L+4M+4N+4O$$
$$= \tfrac{1}{2}(q-3-b),$$

irrespective whether 2 is or is not a fourth power in $\boldsymbol{G}$. Thus the condition for $\boldsymbol{A}, \boldsymbol{B}$ to be complementary difference sets is fulfilled if and only if $b = 0$. But this requires, by the definition of b, that $q = p^{2r}$, $p \equiv 5 \pmod 8$, and Theorem 1 is proved.

References

[1] D. Blatt and G. Szekeres, *A skew Hadamard matrix of order* 52, Canadian J. Math. 21 (1969).

[2] Emma Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod p$, Pacific J. Math. 5 (1955), pp. 103–118.

[3] — *On residue difference sets*, Canadian J. Math. 5 (1953), pp. 425–432.

[4] T. Storer, *Cyclotomy and difference sets*, Chicago 1967.

[5] G. Szekeres, *Tournaments and Hadamard matrices*, L'Enseignement Math. 15 (1969), pp. 269–278.

Received on 25. 3. 1970