

Zeitschrift:	L'Enseignement Mathématique
Herausgeber:	Commission Internationale de l'Enseignement Mathématique
Band:	38 (1992)
Heft:	3-4: L'ENSEIGNEMENT MATHÉMATIQUE
Artikel:	BARKER SEQUENCES AND DIFFERENCE SETS
Autor:	Eliahou, Shalom / Kervaire, Michel
Kapitel:	5. COMMENTS ON THE EXAMPLES IN TABLES II
DOI:	https://doi.org/10.5169/seals-59496

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 19.08.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

The first equation gives

$$P\bar{P} + Q\bar{Q} = 11 + 11(1 + U + \bar{U})(1 + V + \bar{V}).$$

Substituting in the second equation, we get

$$(*) \quad P + \bar{Q} + 5\bar{P}Q + 4P\bar{Q} = -44 + 55(1 + U + \bar{U})(1 + V + \bar{V}).$$

Since $U\bar{U} = 1$, $U^2 = \bar{U}$ and $V\bar{V} = 3 + V + \bar{V}$, $V^2 = V + 2\bar{V}$, the constant terms in $\bar{P}Q$ and $P\bar{Q}$ are equal to $\sum_{i=0}^2 p_i q_i + 3 \sum_{j=3}^8 p_j q_j = c$, say. Hence, equating constant terms in the above equation (*), we must have

$$p_0 + q_0 + 9c = 11.$$

The only solution to this equation with all p_i, q_i being 0 or 1, is $p_0 = q_0 = 1$, $p_i = q_i = 0$ for $i = 1, \dots, 8$. This means $P = Q = 1$, contradicting (*).

5. COMMENTS ON THE EXAMPLES IN TABLES II

Difference sets with parameters $(v, k, \lambda) = (4n - 1, 2n - 1, n - 1)$ are usually called *Hadamard difference sets*. Our purpose here is to discuss the classification of these cyclic difference sets for $2 \leq n \leq 100$.

In many cases where $v = 4n - 1$ is a prime p , the quadratic residue difference set, which we denote by $QR(p)$ is unique for the given values of the parameters. This is obviously the case if the multiplier m has order $k = \frac{1}{2}(v - 1)$ in $(\mathbf{Z}/v\mathbf{Z})^*$. Indeed, in this case, there are exactly 3 orbits of

multiplication by m in $\mathbf{Z}/v\mathbf{Z}$, namely $1 = \{0\}$, $M = \{1, m, m^2, \dots, m^{k-1}\}$ and $\bar{M} = \{-1, -m, \dots, -m^{k-1}\}$. Thus the only choice for D is $D = M$ or $D = \bar{M}$, which are isomorphic under conjugation $\sigma: \mathbf{Z}/v\mathbf{Z} \rightarrow \mathbf{Z}/v\mathbf{Z}$, $\sigma(a) = -a$.

In our Table II, this situation happens for $n = 3, 5, 6, 12, 15, 17, 18, 20, 21, 27, 33, 35, 41, 42, 45, 48, 53, 57, 60, 63, 66, 68, 77, 87, 90$ and 96 .

The remaining cases where $v = 4n - 1$ is a prime p (for $2 \leq n \leq 100$) have been shown to lead to a single difference set, namely $QR(p)$, by machine enumeration of the various choices of D as a union of orbits under multiplication by a multiplier m . This includes the cases $n = 26$ (multiplier 8), $n = 38$ (multiplier 19), $n = 50$ (multiplier 5), $n = 78$ (multiplier 13), $n = 83$ (multiplier 83), and $n = 95$ (multiplier 5). By far, the most difficult case (for the machine) occurs with $n = 38$, which required the examination of 37 442 160 combinations of multiplier orbits.

The case $n = 36$, also leads by machine enumeration to the single difference set $TP(11, 13)$ of twin-prime type with parameters $(143 = 11 \cdot 13, 71, 35)$.

The only other values of $n (\leq 100)$ for which $v = 4n - 1$ is *not* a prime and a Hadamard cyclic difference set with parameters $(4n - 1, 2n - 1, n - 1)$ does exist are powers of 2. The examples for $n = 2, 4$ and 8 are easily seen to be unique.

For $n = 16$, there are 2 isomorphism classes of Hadamard difference sets with parameters $(63, 31, 15)$: Both have multiplier $m = 2$, and denoting by X_a the orbit of a under multiplication by 2 in $\mathbf{Z}/63\mathbf{Z}$, they are

$$D_0 = 1 + X_{-25} + X_{-9} + X_1 + X_3 + X_7 + X_9 ,$$

which is isomorphic to $\mathbf{P}^5(\mathbf{F}_2)$, and

$$D_1 = 1 + X_{-9} + X_{-1} + X_1 + X_3 + X_9 + X_{25} ,$$

which is of type *GMW*.

The difference sets D_0 and D_1 are not isomorphic, even as block designs, as can be seen by computing the cardinalities of the intersection of triples of blocks of D_1 , giving the enumerating polynomial

$$10584t^6 + 19656t^7 + 3528t^8 + 5880t^9 + 63t^{15} ,$$

in contrast to $39060t^7 + 651t^{15}$ for $\mathbf{P}^5(\mathbf{F}_2)$. (The coefficient of t^i being the multiplicity of triple intersections of cardinality i .)

For $n = 32$, L. Baumert and H. Fredricksen have found that there are exactly 6 non-isomorphic examples. (See [BF].) Three of these, $QR(127)$, $\mathbf{P}^6(\mathbf{F}_2)$ and $MH(127)$ are members of the classical families.

For $n = 64$, we have found that there exist exactly 4 examples (up to isomorphism). One of them is $\mathbf{P}^7(\mathbf{F}_2)$, another one is of type *GMW*. The other two seem to be new.

All 4 of them have multiplier 2, which is of order 8 modulo $v = 255$. They all contain the union U of the multiplier orbits of length < 8 , viz.

$$\begin{aligned} U = & \{0\} + \{85, -85\} + \{51, 102, -51, -102\} + \{17, 34, 68, -119\} \\ & + \{-17, -34, -68, 119\} . \end{aligned}$$

Denoting by (a_1, \dots, a_{14}) the union $\sum_{i=1}^{14} X_{a_i}$ of the orbits

$$X_a = \{a, 2a, \dots, 2^7a\} ,$$

the 4 examples are of the form $D_i = U + V_i$, where

$$\begin{aligned}
V_0 &= (-19, -9, -7, -1, 1, 3, 7, 13, 19, 23, 25, 27, 37, 45), \\
V_1 &= (-43, -27, -25, -13, -9, -5, -3, 7, 11, 13, 19, 23, 27, 43), \\
V_2 &= (-43, -27, -23, -13, -11, -3, 1, 3, 7, 13, 15, 25, 37, 43), \\
V_3 &= (-43, -23, -21, -11, -7, -3, 7, 9, 11, 15, 19, 25, 37, 43).
\end{aligned}$$

The difference sets D_2 and D_3 appear to be exotic. D_0 is isomorphic to $\mathbf{P}^7(\mathbf{F}_2)$. Finally, D_1 is of type *GMW*, and can be constructed as follows.

Let $L = \mathbf{F}_{256}$ be the extension of degree 8 over $F = \mathbf{F}_2$. We will use the trace $Tr = Tr_{L/F}: L \rightarrow F$ given by $Tr(\gamma) = \sum_{i=0}^7 \gamma^{2^i}$. The extension L/F is defined by the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1 \in \mathbf{F}[x]$. The multiplicative group \mathbf{F}_{256}^* is generated by any root α of this polynomial. The Hall polynomial $D_0(x)$ of D_0 is then given by

$$D_0(x) = \sum_{i=0}^{254} d_i x^i \in \mathbf{Z}[x]/(x^{255} - 1),$$

where

$$d_i = \begin{cases} 0 & \text{if } Tr(\alpha^i) \neq 0 \\ 1 & \text{if } Tr(\alpha^i) = 0. \end{cases}$$

Thus a block of the difference set is the hyperplane $\ker(Tr) \subset \mathbf{F}_{256} = \mathbf{F}_2^8$.

Under the identification

$$\mathbf{Z}/255\mathbf{Z} \rightarrow \mathbf{F}_{256}^*$$

given by $i \mapsto \alpha^i$, the multiplication by 2 in $\mathbf{Z}/255\mathbf{Z}$ becomes the Frobenius automorphism in the extension $\mathbf{F}_{256}/\mathbf{F}_2$. The block $\ker(Tr)$ is a union of orbits under the action of the multiplier.

In order to construct D_1 , the example of type *GMW*, we need the intermediate extension $K = \mathbf{F}_{16}$, $F \subset K \subset L$. Set $\beta = \alpha^{17}$, a generator of $K^* = \mathbf{F}_{16}^*$. Denote by $tr = tr_{K/F}: K \rightarrow F$ the trace.

Consider the complementary polynomial $D'_0(x) = T - D_0(x)$, where $T = \sum_{i=0}^{254} x^i \in \mathbf{Z}[x]/(x^{255} - 1)$. The crucial point is to observe that $D'_0(x)$ splits as

$$D'_0(x) = \Omega(x) \cdot \theta_0(x^{17}) \in \mathbf{Z}[x]/(x^{255} - 1),$$

where $\theta_0(y) = \sum_{j=0}^{14} a_j y^j$ with

$$a_j = \begin{cases} 0 & \text{if } tr(\beta^j) = 0 \\ 1 & \text{if } tr(\beta^j) \neq 0, \end{cases}$$

and $\Omega(x) = x^7 + x^{14} + \cdots + x^{246}$. Here,

$$\theta_0(y) = y + y^2 + y^3 + y^4 + y^6 + y^8 + y^9 + y^{12}.$$

Now define

$$D'_1(x) = \Omega(x) \cdot \theta_1(x^{17}),$$

where $\theta_1(y) = \theta_0(y^{-1})$. Then $D_1(x) = T - D'_1(x)$ is the Hall polynomial of the difference set D_1 .

The fact that D_0 , D_1 , D_2 and D_3 are not isomorphic, even as block designs, can again be seen by determining the cardinalities of all triple intersections of blocks, for each D_i . Denoting by P_i the corresponding enumerating polynomial of triple intersections for D_i , we have

$$P_0 = 2720340t^{31} + 10795t^{63}$$

$$\begin{aligned} P_1 = & 979200t^{29} + 823140t^{31} + 734400t^{33} + 183600t^{35} \\ & + 10200t^{39} + 595t^{63} \end{aligned}$$

$$\begin{aligned} P_2 = & 9180t^{25} + 8160t^{26} + 45900t^{27} + 163200t^{28} + 342720t^{29} \\ & + 514080t^{30} + 518160t^{31} + 465120t^{32} + 358020t^{33} \\ & + 179520t^{34} + 81090t^{35} + 18360t^{36} + 18360t^{37} + 6120t^{38} \\ & + 3145t^{39} \end{aligned}$$

$$\begin{aligned} P_3 = & 4080t^{25} + 14280t^{26} + 40800t^{27} + 142800t^{28} + 385560t^{29} \\ & + 403920t^{30} + 692580t^{31} + 424320t^{32} + 352920t^{33} + 128520t^{34} \\ & + 79050t^{35} + 32640t^{36} + 9180t^{37} + 12240t^{38} + 7225t^{39} + 1020t^{45}. \end{aligned}$$

TABLE I

Case $\gamma = +1$:

*Non-existence of a cyclic difference set
with parameters $(2t(t+1)+1, t^2, \frac{1}{2}t(t-1))$ for $3 \leq t \leq 100$.
(The case $t=50$ is still undecided.)*

t	(v, k, λ)	$n = k - \lambda$	reason for non-existence
3	(5 ² , 9, 3)	2 · 3	$2^2 \equiv -1 \pmod{5}$
4	(41, 16, 6)	2 · 5	$5^{10} \equiv -1 \pmod{41}$
5	(61, 25, 10)	3 · 5	$3^5 \equiv -1 \pmod{61}$
6	(5 · 17, 36, 15)	3 · 7	$3^2 \equiv -1 \pmod{5}$
7	(113, 49, 21)	$2^2 \cdot 7$	$7^7 \equiv -1 \pmod{113}$
8	(5 · 29, 64, 28)	$2^2 \cdot 3^2$	$2^{14} \equiv -1 \pmod{145}$
9	(181, 81, 36)	$3^2 \cdot 5$	$5 \equiv 3^6 \pmod{181}$ would be multiplier
10	(13 · 17, 100, 45)	5 · 11	$5^2 \equiv -1 \pmod{13}$
11	(5 · 53, 121, 55)	2 · 3 · 11	$2^2 \equiv -1 \pmod{5}$
12	(3 · 13, 144, 66)	2 · 3 · 13	$2^{78} \equiv -1 \pmod{313}$
13	(5 · 73, 169, 78)	7 · 13	$7^2 \equiv -1 \pmod{5}$
14	(421, 196, 91)	3 · 5 · 7	$5^{105} \equiv -1 \pmod{421}$

TABLE I (*continued*)

<i>t</i>	(<i>v</i> , <i>k</i> , λ)	<i>n</i> = <i>k</i> - λ	reason for non-existence
15	(13 · 37, 225, 105)	$2^3 \cdot 3 \cdot 5$	$5^2 \equiv -1 \pmod{13}$
16	(5 · 109, 256, 120)	$2^3 \cdot 17$	$17^2 \equiv -1 \pmod{5}$
17	(613, 289, 136)	$3^2 \cdot 17$	$17^{51} \equiv -1 \pmod{613}$
18	(5 · 137, 324, 153)	$3^2 \cdot 19$	$19 \equiv -1 \pmod{5}$
19	(761, 361, 171)	$2 \cdot 5 \cdot 19$	$2^{190} \equiv -1 \pmod{761}$
20	(29^2 , 400, 190)	$2 \cdot 3 \cdot 5 \cdot 7$	$2^{14} \equiv -1 \pmod{29}$
21	($5^2 \cdot 37$, 441, 210)	$3 \cdot 7 \cdot 11$	$3^2 \equiv -1 \pmod{5}$
22	(1013, 484, 231)	$11 \cdot 23$	$11^{23} \equiv -1 \pmod{1013}$
23	(5 · 13 · 17, 529, 253)	$2^2 \cdot 3 \cdot 23$	$3^2 \equiv -1 \pmod{5}$
24	(1201, 576, 276)	$2^2 \cdot 3 \cdot 5^2$	$3^{150} \equiv -1 \pmod{1201}$
25	(1301, 625, 300)	$5^2 \cdot 13$	$5^{325} \equiv -1 \pmod{1301}$
26	(5 · 281, 676, 325)	$3^3 \cdot 13$	$13^2 \equiv -1 \pmod{5}$
27	(17 · 89, 729, 351)	$2 \cdot 3^3 \cdot 7$	$2^4 \equiv -1 \pmod{17}$
28	($5^3 \cdot 13$, 784, 378)	$2 \cdot 7 \cdot 9$	$2^2 \equiv -1 \pmod{5}$
29	(1741, 841, 406)	$3 \cdot 5 \cdot 29$	$3^{435} \equiv -1 \pmod{1741}$
30	(1861, 900, 435)	$3 \cdot 5 \cdot 31$	$3^{155} \equiv -1 \pmod{1861}$
31	(5 · 397, 961, 465)	$2^4 \cdot 31$	$2^{22} \equiv -1 \pmod{1985}$
32	(2113, 1024, 496)	$2^4 \cdot 3 \cdot 11$	$3^{528} \equiv -1 \pmod{2113}$
33	(5 · 449, 1089, 528)	$3 \cdot 11 \cdot 17$	$3^2 \equiv -1 \pmod{5}$
34	(2381, 1156, 561)	$5 \cdot 7 \cdot 17$	$5^{119} \equiv -1 \pmod{2381}$
35	(2521, 1225, 595)	$2 \cdot 3^2 \cdot 5 \cdot 7$	$2^{630} \equiv -1 \pmod{2521}$
36	(5 · 13 · 41, 1296, 630)	$2 \cdot 3^2 \cdot 37$	$2^2 \equiv -1 \pmod{5}$
37	(29 · 97, 1369, 666)	$19 \cdot 37$	$19^{14} \equiv -1 \pmod{29}$
38	(5 · 593, 1444, 703)	$3 \cdot 13 \cdot 19$	$3^2 \equiv -1 \pmod{5}$
39	(3121, 1521, 741)	$2^2 \cdot 3 \cdot 5 \cdot 13$	$2^{78} \equiv -1 \pmod{3121}$
40	(17 · 193, 1600, 780)	$2^2 \cdot 5 \cdot 41$	$5^8 \equiv -1 \pmod{17}$
41	(5 · 13 · 53, 1681, 820)	$3 \cdot 7 \cdot 41$	$3^2 \equiv -1 \pmod{5}$
42	(3613, 1764, 861)	$3 \cdot 7 \cdot 43$	$3^{903} \equiv -1 \pmod{3613}$
43	(5 · 757, 1849, 903)	$2 \cdot 11 \cdot 43$	$2^2 \equiv -1 \pmod{5}$
44	(17 · 233, 1936, 946)	$2 \cdot 3^2 \cdot 5 \cdot 11$	$2^4 \equiv -1 \pmod{17}$
45	(41 · 101, 2025, 990)	$3^2 \cdot 5 \cdot 23$	$5^{10} \equiv -1 \pmod{41}$
46	($5^2 \cdot 173$, 2116, 1035)	$23 \cdot 47$	$23^2 \equiv -1 \pmod{5}$
47	(4513, 2209, 1081)	$2^3 \cdot 3 \cdot 47$	$3^{188} \equiv -1 \pmod{4513}$
48	(5 · 941, 2304, 1128)	$2^3 \cdot 3 \cdot 7^2$	$3^2 \equiv -1 \pmod{5}$
49	($13^2 \cdot 29$, 2401, 1176)	$5^2 \cdot 7^2$	$5^2 \equiv 7^6 \pmod{4901}$ would be multipli existence unsettled
50	(5101, 2500, 1225)	$3 \cdot 5^2 \cdot 17$	
51	(5 · 1061, 2601, 1275)	$2 \cdot 3 \cdot 13 \cdot 17$	$2^2 \equiv -1 \pmod{5}$
52	(37 · 149, 2704, 1326)	$2 \cdot 13 \cdot 53$	$2^{18} \equiv -1 \pmod{37}$
53	($5^2 \cdot 229$, 2809, 1378)	$3^3 \cdot 53$	$53^2 \equiv -1 \pmod{5}$
54	(13 · 457, 2916, 1431)	$3^3 \cdot 5 \cdot 11$	$5^2 \equiv -1 \pmod{13}$
55	(61 · 101, 3025, 1485)	$2^2 \cdot 5 \cdot 7 \cdot 11$	$5^{15} \equiv -1 \pmod{61}$
56	(5 · 1277, 3136, 1540)	$2^2 \cdot 3 \cdot 7 \cdot 19$	$3^2 \equiv -1 \pmod{5}$
57	(17 · 389, 3249, 1596)	$3 \cdot 19 \cdot 29$	$3^8 \equiv -1 \pmod{17}$

TABLE I (*continued*)

<i>t</i>	(<i>v</i> , <i>k</i> , λ)	<i>n</i> = <i>k</i> - λ	reason for non-existence
58	(5 · 37 ² , 3364, 1653)	29 · 59	$29 \equiv -1 \pmod{5}$
59	(73 · 97, 3481, 1711)	2 · 3 · 5 · 59	$3^6 \equiv -1 \pmod{73}$
60	(7321, 3600, 1770)	2 · 3 · 5 · 61	$2^{610} \equiv -1 \pmod{7321}$
61	(5 · 17, 3721, 1830)	31 · 61	$31^8 \equiv -1 \pmod{17}$
62	(13 · 601, 3844, 1891)	3 ² · 7 · 31	$7^6 \equiv -1 \pmod{13}$
63	(5 · 1613, 3969, 1953)	2 ⁵ · 3 ² · 7	$7^2 \equiv -1 \pmod{5}$
64	(53 · 157, 4096, 2016)	2 ⁵ · 5 · 13	$5^{26} \equiv -1 \pmod{53}$
65	(8581, 4225, 2080)	3 · 5 · 11 · 13	$3^{715} \equiv -1 \pmod{8581}$
66	(5 · 29 · 61, 4356, 2145)	3 · 11 · 67	$3^2 \equiv -1 \pmod{5}$
67	(13 · 701, 4489, 2211)	2 · 17 · 67	$2^6 \equiv -1 \pmod{13}$
68	(5 · 1877, 4624, 2278)	2 · 3 · 17 · 23	$2^2 \equiv -1 \pmod{5}$
69	(9661, 4761, 2346)	3 · 5 · 7 · 23	$7^{2415} \equiv -1 \pmod{9661}$
70	(9941, 4900, 2415)	5 · 7 · 71	$7^{2485} \equiv -1 \pmod{9941}$
71	(5 ² · 409, 5041, 2485)	2 ² · 3 ² · 71	$2^{510} \equiv -1 \pmod{10225}$
72	(10513, 5184, 2556)	2 ² · 3 ² · 73	$2^{1314} \equiv -1 \pmod{10513}$
73	(5 · 2161, 5329, 2628)	37 · 73	$37^2 \equiv -1 \pmod{5}$
74	(17 · 653, 5476, 2701)	3 · 5 ² · 37	$3^8 \equiv -1 \pmod{17}$
75	(13 · 877, 5625, 2775)	2 · 3 · 5 ² · 19	$2^6 \equiv -1 \pmod{13}$
76	(5 · 2341, 5776, 2850)	2 · 7 · 11 · 19	$2^2 \equiv -1 \pmod{5}$
77	(41 · 293, 5929, 2926)	3 · 7 · 11 · 13	$3^4 \equiv -1 \pmod{41}$
78	(5 ² · 17 · 29, 6084, 3003)	3 · 13 · 79	$3^2 \equiv -1 \pmod{5}$
79	(12641, 6241, 3081)	2 ³ · 5 · 79	$5^{1580} \equiv -1 \pmod{12641}$
80	(13 · 997, 6400, 3160)	2 ³ · 3 ⁴ · 5	$5^2 \equiv -1 \pmod{13}$
81	(5 · 2657, 6561, 3240)	3 ⁴ · 41	$41^{332} \equiv -1 \pmod{2657}$
82	(13613, 6724, 3321)	41 · 83	41 ≡ 83 ³ mod 13613 would be multipl
83	(5 · 2789, 6889, 3403)	2 · 3 · 7 · 83	$2^2 \equiv -1 \pmod{5}$
84	(14281, 7056, 3486)	2 · 3 · 5 · 7 · 17	$2^{1190} \equiv -1 \pmod{14281}$
85	(14621, 7225, 3570)	5 · 17 · 43	$5^{3655} \equiv -1 \pmod{14621}$
86	(5 · 41 · 73, 7396, 3655)	3 · 29 · 43	$3^2 \equiv -1 \pmod{5}$
87	(15313, 7569, 3741)	2 ² · 3 · 11 · 29	$3^{1276} \equiv -1 \pmod{15313}$
88	(5 · 13 · 241, 7744, 3828)	2 ² · 11 · 89	$89 \equiv -1 \pmod{5}$
89	(37 · 433, 7921, 3916)	3 ² · 5 · 89	$5^{18} \equiv -1 \pmod{37}$
90	(16381, 8100, 4005)	3 ² · 5 · 7 · 13	$13^{65} \equiv -1 \pmod{16381}$
91	(5 · 17 · 197, 8281, 4095)	2 · 7 · 13 · 23	$2^2 \equiv -1 \pmod{5}$
92	(109 · 157, 8464, 4186)	2 · 3 · 23 · 31	$2^{18} \equiv -1 \pmod{109}$
93	(5 · 13 · 269, 8649, 4278)	3 · 31 · 47	$3^2 \equiv -1 \pmod{5}$
94	(53 · 337, 8836, 4371)	5 · 19 · 47	$5^{26} \equiv -1 \pmod{53}$
95	(17 · 29 · 37, 9025, 4465)	2 ⁴ · 3 · 5 · 19	$3^8 \equiv -1 \pmod{17}$
96	(5 ³ · 149, 9216, 4560)	2 ⁴ · 3 · 97	$3^2 \equiv -1 \pmod{5}$
97	(19013, 9409, 4656)	7 ² · 97	$7^{4753} \equiv -1 \pmod{19013}$
98	(5 · 3881, 9604, 4753)	3 ² · 7 ² · 11	$11^{97} \equiv -1 \pmod{3881}$
99	(19801, 9801, 4851)	2 · 3 ² · 5 ² · 11	$2^{4950} \equiv -1 \pmod{19801}$
100	(20201, 10000, 4950)	2 · 5 ² · 101	$2^{5050} \equiv -1 \pmod{20201}$

TABLE II

Case $\gamma = -1$:Cyclic difference sets with parameters $(4n-1, 2n-1, n-1)$, $2 \leq n \leq 100$

n	$(4n-1, 2n-1, n-1)$	exists?	examples or comment to non-existence
2	(7, 3, 1)	Yes	$P^2(F_2) = QR(7)$
3	(11, 5, 2)	Yes	$QR(11)$
4	(3 · 5, 7, 3)	Yes	$TP(3, 5) = P^3(F_2)$
5	(19, 9, 4)	Yes	$QR(19)$
6	(23, 11, 5)	Yes	$QR(23)$
7	(3 ³ , 13, 6)	No	7 would be multiplier
8	(31, 15, 7)	Yes	$P^4(F_2)$ and $QR(31)$
9	(5 · 7, 17, 8)	Yes	$TP(5, 7)$
10	(3 · 13, 19, 9)	No	$2 \equiv -1 \pmod{3}$
11	(43, 21, 10)	Yes	$QR(43)$
12	(47, 23, 11)	Yes	$QR(47)$
13	(3 · 17, 25, 12)	No	$13^2 \equiv -1 \pmod{17}$
14	(5 · 11, 27, 13)	No	$2^2 \equiv -1 \pmod{5}$
15	(59, 29, 14)	Yes	$QR(59)$
16	(3 ² · 7, 31, 15)	Yes	$P^5(F_2)$ and GMW
17	(67, 33, 16)	Yes	$QR(67)$
18	(71, 35, 17)	Yes	$QR(71)$
19	(3 · 5 ² , 35, 18)	No	$19 \equiv -1 \pmod{5}$
20	(79, 39, 19)	Yes	$QR(79)$
21	(83, 41, 20)	Yes	$QR(83)$
22	(3 · 29, 43, 21)	No	$2 \equiv -1 \pmod{3}$
23	(7 · 13, 45, 22)	No	$23^3 \equiv -1 \pmod{13}$
24	(5 · 19, 47, 23)	No	$3^2 \equiv -1 \pmod{5}$
25	(3 ² · 11, 49, 24)	No	25 would be multiplier
26	(103, 51, 25)	Yes	$QR(103)$
27	(107, 53, 26)	Yes	$QR(107)$
28	(3 · 37, 55, 27)	No	$m = 7 \equiv 2^{32}$ would be multiplier
29	(5 · 23, 57, 28)	No	$29 \equiv -1 \pmod{5}$
30	(7 · 17, 59, 29)	No	$2^4 \equiv -1 \pmod{17}$
31	(3 · 41, 61, 30)	No	$31^5 \equiv -1 \pmod{41}$
32	(127, 63, 31)	Yes	$P^6(F_2)$, $QR(127)$, $MH(127)$, and 3 others
33	(131, 65, 32)	Yes	$QR(131)$
34	(3 ³ · 5, 67, 33)	No	$17 \equiv -1 \pmod{3}$
35	(139, 69, 34)	Yes	$QR(139)$
36	(11 · 13, 71, 35)	Yes	$TP(11, 13)$
37	(3 · 7 ² , 73, 36)	No	37 would be multiplier
38	(151, 75, 37)	Yes	$QR(151)$
39	(5 · 31, 77, 38)	No	$3^2 \equiv -1 \pmod{5}$
40	(3 · 53, 79, 39)	No	$5 \equiv -1 \pmod{3}$

TABLE 2 (*continued*)

n	$(4n - 1, 2n - 1, n - 1)$	exists?	examples or comment to non-existence
41	(163, 81, 40)	Yes	$QR(163)$
42	(167, 83, 41)	Yes	$QR(167)$
43	($3^2 \cdot 19$, 85, 42)	No	43 would be multiplier
44	($5^2 \cdot 7$, 87, 43)	No	$m = 11 \equiv 2^{56} \pmod{175}$ would be multiplier
45	(179, 89, 44)	Yes	$QR(179)$
46	(3 · 61, 91, 45)	No	$23 \equiv -1 \pmod{3}$
47	(11 · 17, 93, 46)	No	$47^2 \equiv -1 \pmod{17}$
48	(191, 95, 47)	Yes	$QR(191)$
49	(3 · 5 · 13, 97, 48)	No	7 would be multiplier
50	(199, 99, 49)	Yes	$QR(199)$
51	(7 · 29, 101, 50)	No	$3^3 \equiv -1 \pmod{7}$
52	($3^2 \cdot 23$, 103, 51)	No	13 would be multiplier
53	(211, 105, 52)	Yes	$QR(211)$
54	(5 · 43, 107, 53)	No	$2^2 \equiv -1 \pmod{5}$
55	(3 · 73, 109, 54)	No	$5 \equiv -1 \pmod{3}$
56	(223, 111, 55)	Yes	$QR(223)$ and $MH(223)$
57	(227, 113, 56)	Yes	$QR(227)$
58	(3 · 7 · 11, 115, 57)	No	$2 \equiv -1 \pmod{3}$
59	(5 · 47, 117, 58)	No	$59 \equiv -1 \pmod{5}$
60	(239, 119, 59)	Yes	$QR(239)$
61	(3^5 , 121, 60)	No	61 would be multiplier
62	(13 · 19, 123, 61)	No	$2^6 \equiv -1 \pmod{13}$
63	(251, 125, 62)	Yes	$QR(251)$
64	(3 · 5 · 17, 127, 63)	Yes	$\mathbf{P}^7(\mathbf{F}_2)$, GMW and 2 new ones
65	(7 · 37, 129, 64)	No	$5^3 \equiv -1 \pmod{7}$
66	(263, 131, 65)	Yes	$QR(263)$
67	(3 · 89, 133, 66)	No	67 would be multiplier
68	(271, 135, 67)	Yes	$QR(271)$
69	($5^2 \cdot 11$, 137, 68)	No	$3^2 \equiv -1 \pmod{5}$
70	($3^2 \cdot 31$, 139, 69)	No	$2 \equiv -1 \pmod{3}$
71	(283, 141, 70)	Yes	$QR(283)$ and $MH(283)$
72	(7 · 41, 143, 71)	No	$m = 9 \equiv 2^{55} \equiv 3^2 \pmod{287}$ would be multiplier
73	(3 · 97, 145, 72)	No	$73^{12} \equiv -1 \pmod{97}$
74	(5 · 59, 147, 73)	No	$2^2 \equiv -1 \pmod{5}$
75	(13 · 23, 149, 74)	No	$m = 3^3 \equiv 5^4 \pmod{299}$ would be multiplier
76	(3 · 101, 151, 75)	No	$m = 19 \equiv 2^9 \pmod{303}$ would be multiplier
77	(307, 153, 76)	Yes	$QR(307)$
78	(311, 155, 77)	Yes	$QR(311)$
79	($3^2 \cdot 5 \cdot 7$, 157, 78)	No	$79 \equiv -1 \pmod{5}$
80	(11 · 29, 159, 79)	No	$5^7 \equiv -1 \pmod{29}$
81	(17 · 19, 161, 80)	Yes	$TP(17, 19)$
82	(3 · 109, 163, 81)	No	$2 \equiv -1 \pmod{3}$

TABLE II (*continued*)

n	$(4n - 1, 2n - 1, n - 1)$	exists?	examples or comment to non-existence
83	(331, 165, 82)	Yes	$QR(331)$
84	(5 · 67, 167, 83)	No	$3^2 \equiv -1 \pmod{5}$
85	(3 · 113, 169, 84)	No	$5 \equiv -1 \pmod{3}$
86	(7 ³ , 171, 85)	No	$m = 43 \equiv 2^{144} \pmod{343}$ would be multiplier
87	(347, 173, 86)	Yes	$QR(347)$
88	(3 ³ · 13, 175, 87)	No	$11 \equiv -1 \pmod{3}$
89	(5 · 71, 177, 88)	No	$89 \equiv -1 \pmod{5}$
90	(359, 179, 89)	Yes	$QR(359)$
91	(3 · 11 ² , 181, 90)	No	$7^5 \equiv -1 \pmod{11}$
92	(367, 183, 91)	Yes	$QR(367)$
93	(7 · 53, 185, 92)	No	$3^3 \equiv -1 \pmod{7}$
94	(3 · 5 ³ , 187, 93)	No	$2 \equiv -1 \pmod{3}$
95	(379, 189, 94)	Yes	$QR(379)$
96	(383, 191, 95)	Yes	$QR(383)$
97	(3 ² · 43, 193, 96)	No	97 would be multiplier
98	(17 · 23, 195, 97)	No	$2^4 \equiv -1 \pmod{17}$
99	(5 · 79, 197, 98)	No	$11 \equiv 3^{68} \pmod{395}$ would be multiplier
100	(3 · 7 · 19, 199, 99)	No	$4 = 2^2 \equiv 5^8 \pmod{399}$ would be multiplier

REFERENCES

- [Bar] BARKER, R. H. Group synchronizing of binary digital systems. In *Communication Theory*, W. Jackson, Ed., London: Butterworth, 1953, pp. 273-287.
- [Bau] BAUMERT, L. D. *Cyclic difference sets*. Lecture Notes in Mathematics 182, New York: Springer-Verlag, 1971.
- [BF] BAUMERT, L. D. and H. FREDRICKSEN. The Cyclotomic Numbers of Order Eighteen with Applications to Difference Sets. *Math. Comp.* 21 (1967), 204-219.
- [EKS] ELIAHOU, S., M. KERVAIRE and B. SAFFARI. A New Restriction on the Lengths of Golay Complementary Sequences. *J. Comb. Theory., Ser. A* 55 (1990), 45-59.
- [GMW] GORDON, B., W. H. MILLS and L. R. WELCH. Some New Difference Sets. *Canad. J. Math.* 14 (1962), 614-625.
- [H] HALL, M. Jr. *Combinatorial Theory*. Wiley-Interscience, Second Edition, 1986.
- [JL] JEDWAB, J. and S. LLOYD. A Note on the Nonexistence of Barker Sequences. *Designs, Codes and Cryptography* 2 (1992), 93-97.
- [L] LANDER, E. S. *Symmetric Designs: An Algebraic Approach*. London Math. Soc. Lecture Note Series 74, Cambridge University Press, 1983.