International Scholarly Research Network
ISRN Algebra
Volume 2012, Article ID 367129, 19 pages
doi:10.5402/2012/367129

Research Article

On the Existence of (v, k, λ) Difference Sets with $k < 1250$ and $k - \lambda$ Is a Square

Adegoke Solomon Osifodunrin

Division of Sciences and Mathematics, Department of Mathematics, Livingstone College, Salisbury, NC 28144, USA

Correspondence should be addressed to
Adegoke Solomon Osifodunrin, asa_osifodunrin@yahoo.com

Received 20 January 2012; Accepted 8 February 2012

Academic Editors: A. V. Kelarev, D. Kressner, H. You, and A. Zimmermann

We combine Turyn's self-conjugacy result, variance technique, Dillon dihedral trick, and Sylow theorem to investigate the existence of (v, k, λ) difference sets in which $k - \lambda$ is a square and $k < 1250$.

1. Introduction

Let G be a multiplicative group of order v and let D be a subset of G consisting of k elements, where $1 < k < v - 1$. D is a nontrivial (v, k, λ) difference set if every nonidentity element can be reproduced λ times by the multiset $\{d_1 d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2\}$. The natural number $n = k - \lambda > 1$ is known as the order of the difference set. The group structure determines the nature of the difference set. For instance, if the underlying group G is abelian (resp., nonabelian or cyclic), then D is abelian (resp., nonabelian or cyclic) difference set. The study of difference sets integrates various techniques ranging from algebraic number theory to geometry, algebra, and combinatorics [1]. There are many classical results on constructions and nonexistence of difference sets in the literature [2–14]. These results are mainly based on Hall's multiplier concept [15] or Turyn's self-conjugacy method [14]. Recently, Schmidt [13] developed a new method for studying combinatorial structures using group ring equations without any restrictive assumptions. Arasu [2], Arasu and Sehgal [3, 16], Baumert [4], Hughes [17], Iiams [7], Kibler [18], Kopilovich [10], Lander [11], and López and Sánchez [19] among other authors studied the existence of abelian (v, k, λ) difference sets with $k \leq 150$. They were able to either indicate the existence or otherwise of difference sets. Some of these authors also listed parameter sets that were open, whose existence or otherwise has been

concluded by other authors. This paper mainly uses Turyn's self-conjugacy approach to study a class of (v, k, λ) difference sets in which $n = m^2$, where m is a positive integer. We illustrate with examples where $2 \leq m \leq 25$ and the ideal generated by prime divisors of m factors *trivially* in the respective cyclotomic rings. This assumption along with Dillon dihedral trick and Sylow theorems provide sufficient information required to decide the nonesxistence of the difference sets in some or all groups of order v.

We assume that G is a finite group of order v. Section 2 gives a brief description of some basic results which include materials from group theory, representation, and algebraic number theories. Section 3 lists difference sets parameters that do not exist and examples of partial results of nonexistence of difference sets in groups of order v.

2. Preliminaries

2.1. Difference Sets

Let $\mathbb{Z}$ be the ring of integers and $\mathbb{C}$ be the field of complex numbers. Suppose that G is a group of order v and D is a (v, k, λ) difference set in G. We sometimes view the elements of D as members of the group ring $\mathbb{Z}[G]$, which is a subring of the group algebra $\mathbb{C}[G]$. Thus, D represents both subset of G and element $\sum_{g\in D} g$ of $\mathbb{Z}[G]$. The sum of inverses of elements of D is $D^{(-1)} = \sum_{g\in D} g^{-1}$. Consequently, D is a difference set if and only if

$$DD^{(-1)} = n + \lambda G, \qquad DG = kG. \tag{2.1}$$

Suppose that D is a difference set in a group G of order v and N is a normal subgroup of G. Suppose that $\psi : G \to G/N$ is a homomorphism. We can extend ψ by linearity, to the corresponding group rings. Thus, the difference set image in G/N (also known as the contraction of D with respect to the kernel N) is the multiset $D/N = \psi(D) = \{dN : d \in D\}$. Let $T^* = \{1, t_1, \ldots, t_h\}$ be a left transversal of N in G. We can write $\psi(D) = \sum_{t_j\in T^*} d_j t_j N$, where the integer $d_j = |D \cap t_j N|$ is known as the *intersection number* of D with respect to N. In this work, we will always use the notation $\widehat{D}$ for $\psi(D)$ and $m_i \geq 0$ denotes the number of times d_i equals i.

2.2. Representation and Algebraic Number Theories

A $\mathbb{C}$-representation of G is a homomorphism, $\chi : G \to \mathrm{GL}(d, \mathbb{C})$, where $\mathrm{GL}(d, \mathbb{C})$ is the group of invertible $d \times d$ matrices over $\mathbb{C}$. The positive integer d is the degree of χ. A linear representation (character) is a representation of degree one. The set of all linear representations of G is denoted by G^*. G^* is an abelian group under multiplication and if G' is the derived group of G, then G^* is isomorphic to G/G'. Define $\zeta_{m'} := e^{(2\pi/m')i}$ to be a primitive m'th root of unity and $K_{m'} := \mathbb{Q}(\zeta_{m'})$ to be the cyclotomic extension of the field of rational numbers, $\mathbb{Q}$, where m' is the exponent of G. Without loss of generality, we may replace $\mathbb{C}$ by the field $K_{m'}$. Thus, the central primitive idempotents in $\mathbb{C}[G]$ is

$$e_{\chi_i} = \frac{\chi_i(1)}{|G|} \sum_{g\in G} \chi_i(g) g^{-1} = \frac{1}{|G|} \sum_{g\in G} \overline{\chi_i(g)} g, \tag{2.2}$$

where χ_i is an irreducible character of G.

Aliases are members of group ring which enable us to transfer information from $\mathbb{C}[G]$ to group algebra $\mathbb{Q}[G]$ and then to $\mathbb{Z}[G]$. Let G be an abelian group and let $\Omega = \{\chi_1, \chi_2, \ldots, \chi_h\}$, be the set of characters of G. The element $\beta \in \mathbb{Z}[G]$ is known as Ω-*alias* if for $A \in \mathbb{Z}[G]$ and all $\chi_i \in \Omega$, $\chi_i(A) = \chi_i(\beta)$. Since $A = \sum_{\chi \in G^*} \chi(A) e_\chi$, we can replace the occurrence of $\chi(A)$, which is a complex number by Ω-alias, β, an element of $\mathbb{Z}[G]$. Furthermore, two characters of G are algebraic conjugate if and only if they have the same kernel and we denote the set of equivalence classes of G^* by $G^*/\sim$. The *central rational idempotents* in $\mathbb{Q}[G]$ are obtained by summing over the equivalence classes $X_i = \{e_{\chi_i} \mid \chi_i \sim \chi_j\} \in G^*/\sim$ on the e_χ's under the action of the Galois group of $K_{m'}$ over $\mathbb{Q}$. That is, $[e_{\chi_i}] = \sum_{e_{\chi_j} \in X_i} e_{\chi_j}$, $i = 1, \ldots, s$.

For instance, suppose $G = C_{p^{m'}} = \langle x : x^{p^{m'}} = 1 \rangle$ (p is prime) is a cyclic group whose characters are of the form $\chi_i(x) = \zeta^i_{p^{m'}}$, $i = 0, \ldots, p^{m'} - 1$. Then the rational idempotents are

$$\begin{aligned} \left[e_{\chi_0}\right] &= \frac{1}{p^{m'}} \langle x \rangle, \\ \left[e_{\chi_{p^j}}\right] &= \frac{1}{p^{j+1}} \left(p \left\langle x^{p^{m'-j}} \right\rangle - \left\langle x^{p^{m'-j-1}} \right\rangle \right), \quad 0 \le j \le m' - 1. \end{aligned} \tag{2.3}$$

The following is the general formula employed in the search of difference set [22].

Theorem 2.1. *Let G be an abelian group and $G^*/\sim$ be the set of equivalence classes of characters. Suppose that $\{\chi_0, \chi_1, \ldots, \chi_s\}$ is a system of distinct representatives for the equivalence classes of $G^*/\sim$. Then for $A \in \mathbb{Z}[G]$, one has*

$$A = \sum_{i=0}^{s} \alpha_i \left[e_{\chi_i}\right], \tag{2.4}$$

where α_i is any χ_i-alias for A.

Equation (2.4) is known as *the rational idempotent decomposition* of A.

Suppose that χ is any nontrivial representation of degree d and $\chi(\widehat{D}) \in \mathbb{Z}[\zeta]$, where ζ is the primitive root of unity. Suppose that $x \in G$ is a nonidentity element. Then, $\chi(xG) = \chi(x)\chi(G) = \chi(G)$. This shows that $(\chi(x) - 1)\chi(G) = 0$. Since x is not an identity element, $(\chi(x) - 1) \neq 0$ and $\chi(G) = 0$ ($\mathbb{Z}[\zeta]$ is an integral domain). Consequently, $\chi(D)\overline{\chi(D)} = n \cdot I_d + \lambda\chi(G) = n \cdot I_d$, where I_d is the $d \times d$ identity matrix. Furthermore, if χ is a nontrivial representation of G/N of degree d then $\widehat{D}\widehat{D}^{(-1)} = n \cdot 1_{G/N} + |N|\lambda(G/N)$ and $\chi(\widehat{D})\overline{\chi(\widehat{D})} = n \cdot I_d$.

Recall that the ring of integers of the cyclotomic field $\mathbb{Q}[\zeta_{m'}]$ is $\mathbb{Z}[\zeta_{m'}]$. This ring is also an integral domain. Let $p, a, b \in \mathbb{Z}[\zeta_{m'}]$. The number p is irreducible if $p = ab$ implies one of a or b is a unit. The element p is prime if $p \mid ab$ implies $p \mid a$ or $p \mid b$ [23]. A domain is a unique factorization domain (UFD) if factorization into irreducibles is possible and unique. In UFD, the irreducibles are also primes. In order to successfully obtain the difference set images, we need the aliases. Suppose that G/N is an abelian factor group of exponent m' and $\widehat{D}$ is a difference set image in G/N. If χ is not a principal character of G/N, then $\chi(\widehat{D})\overline{\chi(\widehat{D})} = n$ is an algebraic equation in $\mathbb{Z}[\zeta_{m'}]$. The determination of the alias requires the knowledge of how the ideal generated by $\chi(\widehat{D})$ factors in cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, where $\zeta_{m'}$ is the m'th root of unity. If $\delta := \chi(\widehat{D})$, then by (2.4), we seek $\alpha \in \mathbb{Z}[G/N]$ such that $\chi(\alpha) = \delta$. The task of solving

the algebraic equation $\delta\overline{\delta} = n$ is sometimes made easier if we consider the factorization of principal ideals $\langle\delta\rangle\langle\overline{\delta}\rangle = \langle n\rangle$. Suppose we are able to find $\delta = \sum_{i=0}^{\phi(m')-1} d_i\zeta_{m'}^i \in \mathbb{Z}[\zeta_{m'}]$ such that $\delta\overline{\delta} = n$, where ϕ is the Euler ϕ-function. A theorem due to Kronecker [12, 13] states that any algebraic integer whose all conjugates have absolute value 1 must be a root of unity. We use this theorem to characterize the solutions. If there is any other solution to the algebraic equation, then it must be of the form $\delta' = \delta u$, where $u = \pm\zeta_{m'}^j$ is a unit.

The following result is used to determine the number of factors of an ideal in a ring: suppose p is any prime and m' is an integer such that $\gcd(p, m') = 1$. Suppose that d is the order of p in the multiplicative group $\mathbb{Z}_{m'}^*$ of the modular number ring $\mathbb{Z}_{m'}$. Then the number of prime ideal factors of the principal ideal $\langle p\rangle$ in the cyclotomic integer ring $\mathbb{Z}[\zeta_{m'}]$ is $\phi(m')/d$, where ϕ is the Euler ϕ-function, that is, $\phi(m') = |\mathbb{Z}_{m'}^*|$ [25]. For instance, the ideal generated by 2 has two factors in $\mathbb{Z}[\zeta_7]$, the ideal generated by 7 has two factors in $\mathbb{Z}[\zeta_{20}]$, while the ideal generated by 3 has four factors in $\mathbb{Z}[\zeta_{40}]$. On the other hand, since 2^s is a power of 2, the ideal generated by 2 is said to completely ramifies as power of $\langle 1 - \zeta_{2^s}\rangle = \overline{\langle 1 - \zeta_{2^s}\rangle}$ in $\mathbb{Z}[\zeta_{2^s}]$.

According to Turyn [14], an integer n is said to be semi-primitive modulo m' if for every prime factor p of n, there is an integer i such that $p^i \equiv -1 \bmod m'$. In this case, -1 belongs to the multiplicative group generated by p. Furthermore, n is self-cosnjugate modulo m' if every prime divisor of n is semi primitive modulo m'_p, where m'_p is the largest divisor of m' relatively prime to p. This means that all prime ideals over n in $\mathbb{Z}[\zeta_{m'}]$ are fixed by complex conjugation. For instance, $7^2 \equiv -1 \pmod{m'}$, where $m' = 2, 5, 10$ and $7 \equiv -1 \pmod{m'}$, $m' = 2, 4, 8$. Thus, $\langle 7\rangle$ is fixed by conjugation in $\mathbb{Z}[\zeta_{m'}]$, $m' = 2, 4, 5, 8, 10, 50$.

Remark 2.2. If $\langle n\rangle = \Pi_{i=1}^s\theta_i$ in cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, where θ_i is an ideal and s is an odd integer, then there is no solution to $\delta\overline{\delta} = n$. To see this, assume that a δ exist such that $\langle\delta\rangle = \Pi_{i=1}^k\alpha_i$. Then $\langle n\rangle = \langle\delta\rangle\langle\overline{\delta}\rangle$ has $2k$ factors but $\langle n\rangle$ has odd factors.

Remark 2.3. Let us consider the ideal generated by 2 which has two factors in the cyclotomic ring $\mathbb{Z}[\zeta_{23}]$. We claim that the algebraic number 2 is prime in this ring. Since (23, 11, 5) difference sets exist, and there exists θ such that $\theta\overline{\theta} = 6$ and $\theta + \overline{\theta} = -1$. This implies that $\theta^2 + \theta + 6 = 0$ and $\theta = (-1 \pm \sqrt{-23})/2$. Consequently, $\theta \in \mathbb{Z}[\sqrt{-23}]$. Suppose that the algebraic number 2 is not prime in $\mathbb{Z}[\sqrt{-23}]$. As $-23 \equiv 1 \,(\mathrm{mod}\, 4)$ ([23], chapter 3), we seek $a, b \in \mathbb{Z}$ such that $\delta = (a + b\sqrt{-23})/2$ and $\delta\overline{\delta} = (a^2 + 23b^2)/4 = 2$. The equation $a^2 + 23b^2 = 8$ has no integer solution. Thus, there is no algebraic number such that $\delta\overline{\delta} = 2$. In fact, $\delta\overline{\delta} = p$ has no solution, where $p = 2, 3, 5, 7, 10, 11, 13, 14, 15, 17, 19, 20, 21, 22$. However, the equation $a^2 + 23b^2 = 4m^2$ has trivial solutions $(a, b) = (-2m, 0)$ and $(2m, 0)$, where $m = 2, 3, 4, 5, 7, 9, 10, 11, 13, 14, 15, 17, 19, 20, 21, 22, 25$. We noticed that since the class number of the cyclotomic ring $\mathbb{Z}[\zeta_{23}]$ is 3, the equation $a^2 + 23b^2 = 4 \cdot 2^3$ has nontrivial solutions $(a, b) = (-3, -1)$, $(-3, 1)$, $(3, -1)$ and $(3, 1)$. Also, $a^2 + 23b^2 = 4m$ has nontrivial solutions for $m = 6, 8, 12, 18, 6^2, 8^2, 12^2, 16^2, 18^2$ and 24^2.

In this paper, we will use the phase *m factors trivially* in $\mathbb{Z}[\zeta_{m'}]$ if the ideal generated by m is prime or ramifies in $\mathbb{Z}[\zeta_{m'}]$; m is self-conjugate modulo m'; the ideal generated by m has odd factors or the algebraic equation $\delta\overline{\delta} = m^2$ has no solution or has trivial solutions. In summary, suppose that $\widehat{D}$ is the difference set image of order $n = m^2$ in the cyclic factor group G/N, where G/N is a group with exponent m'. Suppose that m factors trivially in $\mathbb{Z}[\zeta_{m'}]$ and χ is a nontrivial representation of G/N. Then $\chi(\widehat{D}) = \pm m\zeta_{m'}^i$, $\zeta_{m'}$ is the m'th root of unity [13].

2.3. Characteristics of Difference Set Images in Subgroup of a Group

In this subsection, we use the attributes of subgroups of a group to obtain information about the difference set image in the subgroups. Dillon [5] proved the following results which will be used to obtain difference set images in dihedral group of a certain order if the difference images in the cyclic group of same order are known.

Theorem 2.4 (dillon dihedral trick). *Let H be an abelian group and let G be the generalized dihedral extension of H. That is, $G = \langle q, H : q^2 = 1, qhq = h^{-1}, \forall h \in H \rangle$. If G contains a difference set, then so does every abelian group which contains H as a subgroup of index 2.*

Corollary 2.5. *If the cyclic group Z_{2m} does not contain a (nontrivial) difference set, then neither does the dihedral group of order $2m$.*

Remark 2.6. We look at subgroup properties of a group that can aid the construction of difference set image. For the convenience of the reader, we reproduce the idea of Gjoneski et al. [26]. Suppose that H is a group of order $2h$ with a central involution z. We take $T = \{t_i : i = 1, \ldots, h\}$ to be the transversal of $\langle z \rangle$ in H so that every element in H is viewed as $t_i z^j$, $0 \leq i \leq h$, $j = 0, 1$. Denote the set of all integral combinations, $\sum_{i=1}^{h} a_i t_i$ of elements of T, $a_i \in \mathbb{Z}$ by $\mathbb{Z}[T]$. Using the two representations of subgroup $\langle z \rangle$ and Frobenius reciprocity theorem [27], we may write any element X of the group ring $\mathbb{Z}[H]$ in the form

$$X = X\left(\frac{1+z}{2}\right) + X\left(\frac{1-z}{2}\right). \tag{2.5}$$

Furthermore, let A be the group ring element created by replacing every occurrence of z in X by 1. Also, let B be the group ring element created by replacing every occurrence of z in H by -1. Then

$$X = A\left(\frac{\langle z \rangle}{2}\right) + B\left(\frac{2 - \langle z \rangle}{2}\right), \tag{2.6}$$

where $A = \sum_{i=1}^{h} a_i t_i$ and $B = \sum_{j=1}^{h} b_j t_j$, $a_i, b_j \in \mathbb{Z}$. As $X \in \mathbb{Z}[H]$, A and B are both in $\mathbb{Z}[T]$, and $A \equiv B \bmod 2$. We may equate A with the homomorphic image of X in $G/\langle z \rangle$. Consequently, if X is a difference set, then the coefficients of t_i in the expression for A will be intersection number of X in the coset $\langle z \rangle$ [26]. In particular, it can be shown that if K is a subgroup of a group H such that

$$H \cong K \times \langle z \rangle, \tag{2.7}$$

then the difference set image in H is

$$\widehat{D} = A\left(\frac{\langle z \rangle}{2}\right) + gB\left(\frac{2 - \langle z \rangle}{2}\right), \tag{2.8}$$

where $g \in H$, A is a difference set in K, $\alpha = (k+m)/|K|$ or $\alpha = (k-m)/|K|$, $B = A - \alpha K$ and k is the size of the difference set. Equation (2.8) is true as long as $|K| \mid (k+m)$ or $|K| \mid (k-m)$.

Table 1: Parameter sets that do not exist by Criterion 1. $C_{|G/N|} = \langle x \rangle$ and parameters with asterisk indicate new results.

	(v, k, λ)	m	p	$\lvert G/N \rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert G/N \rvert}]$	No. of groups of order v	Solutions in G/N
1	(115, 19, 3)	4	2	23	Remark 2.3	1	$-4 + \langle x \rangle$
2	(1333, 37, 1)	6	2, 3	43	$a \equiv -1 (\mathrm{mod} 43)$ $a = 2^7, 3^{21}$	1	$-6 + \langle x \rangle$
3	(221, 45, 9)	6	2, 3	17	$a \equiv -1 \pmod{17}$ $a = 2^4, 3^8$	1	$-6 + 3\langle x \rangle$
4	(145, 64, 28)	6	2, 3	29	$a^{14} \equiv -1 \pmod{29}$, $a = 2, 3$	1	$6 + 2\langle x \rangle$
5	(1463, 86, 5)	9	3	19	$3^9 \equiv -1 \pmod{19}$	1	$-9 + 5\langle x \rangle$
6	(583, 97, 16)	9	3	53	$3^{26} \equiv -1 \pmod{53}$	1	$-9 + 2\langle x \rangle$
7	(345, 129, 48)	9	3	23	Remark 2.3	1	$-9 + 6\langle x \rangle$
8	(3503, 103, 3)	10	2, 5	113	$a \equiv -1 \pmod{113}$ $a = 2^{14}, 5^{56}$	1	$-10 + \langle x \rangle$
9	(2185, 105, 5)	10	2, 5	23	Remark 2.3	1	$-10 + 5\langle x \rangle$
10	(1309, 109, 9)	10	2, 5	17	$a \equiv -1 \pmod{17}$ $a = 2^4, 5^8$	1	$-10 + 7\langle x \rangle$
11	(1037, 112, 12)	10	2, 5	61	$a \equiv -1 \pmod{61}$ $a = 2^{30}, 5^{15}$	1	$-10 + 2\langle x \rangle$
12*	(621, 125, 25)	10	2, 5	69	$5^{11} \equiv -1 \pmod{b}$ $b = 23, 69$ 2 factors trivially in $\mathbb{Z}[\zeta_a]$, $a = 23, 69$	5	$10 + 5\langle x \rangle$ in C_{23}; None in C_{69}
13	(469, 144, 44)	10	2, 5	67	$a \equiv -1 \pmod{67}$ $a = 2^{33}, 5^{11}$	1	$10 + 2\langle x \rangle$
14	(407, 175, 75)	10	2, 5	37	$a^{18} \equiv -1 \pmod{37}$ $a = 2, 5$	1	$-10 + 5\langle x \rangle$
15	(3151, 126, 5)	11	11	137	$11^{34} \equiv -1 \pmod{137}$	1	$-11 + \langle x \rangle$
16*	(483, 241, 120)	11	11	23	$11^{11} \equiv -1 \pmod{b}$ $b = 23, 69$	2	$11 + 10\langle x \rangle$ in C_{23}; None in C_{69}
17	(561, 176, 55)	11	11	187	$11^8 \equiv -1 (\mathrm{mod} 17)$ 11 factors trivially in $\mathbb{Z}[\zeta_a]$, $a = 17, 187$	1	$-11 + 11\langle x \rangle$ in C_{17}; None in C_{187}
18	(20881, 145, 1)	12	2, 3	157	$a \equiv -1 \pmod{157}$ $a = 2^{26}, 3^{39}$	1	$-12 + \langle x \rangle$
19	(1591, 160, 16)	12	2, 3	43	$a \equiv -1 \pmod{43}$ $a = 2^7, 3^{21}$	1	$-12 + 4\langle x \rangle$
20	(9805, 172, 3)	13	13	37	$13^{18} \equiv -1 \pmod{37}$	1	$-13 + 5\langle x \rangle$
21*	(3895, 177, 8)	13	13	19	$13^9 \equiv -1 \pmod{19}$	2	$-13 + 10\langle x \rangle$
22*	(1711, 190, 21)	13	13	29	$13^7 \equiv -1 \pmod{29}$	2	$-13 + 7\langle x \rangle$
23	(2323, 216, 20)	14	14	23	$14^{11} \equiv -1 \pmod{23}$	1	$-14 + 10\langle x \rangle$
24*	(9951, 200, 4)	14	2, 7	107	$a^{53} \equiv -1 \pmod{107}$ $a = 2, 7$	2	$-14 + 2\langle x \rangle$
25	(8041, 201, 5)	14	2, 7	43	$a \equiv -1 \pmod{43}$ $a = 2^7, 7^3$	1	$-14 + 5\langle x \rangle$
26	(793, 352, 156)	14	2, 7	61	$a^{30} \equiv -1 \pmod{61}$ $a = 2, 7$	1	$-14 + 6\langle x \rangle$
27	(50851, 226, 1)	15	3, 5	241	$a \equiv -1 \pmod{241}$ $a = 3^{60}, 5^{20}$	1	$-15 + \langle x \rangle$

Table 1: Continued.

	(v, k, λ)	m	p	$\lvert G/N\rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert G/N\rvert}]$	No. of groups of order v	Solutions in G/N
28*	(2871, 246, 21)	15	3, 5	29	$a \equiv -1 \pmod{29}$ $a = 3^{14}, 5^{7}$	2	$-15 + 9\langle x\rangle$
29	(2491, 250, 25)	15	3, 5	53	$a^{26} \equiv -1 \pmod{53}$ $a = 3, 5$	1	$-15 + 5\langle x\rangle$
30*	(13573, 261, 5)	16	2	277	$2^{46} \equiv -1 \pmod{277}$	2	$-16 + \langle x\rangle$
31	(4879, 271, 15)	16	2	41	$2^{10} \equiv -1 \pmod{41}$	1	$-16 + 7\langle x\rangle$
32*	(26815, 328, 4)	18	2, 3	173	$a^{86} \equiv -1 \pmod{173}$ $a = 2, 3$	2	$-18 + 2\langle x\rangle$
33*	(4551, 351, 27)	18	2, 3	41	$a \equiv -1 \pmod{41}$ $a = 2^{10}, 3^{4}$	2	$-18 + 9\langle x\rangle$
34*	(16975, 369, 8)	19	19	97	$19^{16} \equiv -1 \pmod{97}$	2	$-19 + 4\langle x\rangle$
35*	(15171, 370, 9)	19	19	389	$19^{97} \equiv -1 \pmod{389}$	2	$-19 + \langle x\rangle$
36	(2599, 433, 72)	19	19	113	$19^{56} \equiv -1 \pmod{113}$	1	$-19 + 4\langle x\rangle$
37	(11455, 415, 15)	20	2, 5	29	$a \equiv -1 \pmod{29}$ $a = 2^{14}, 5^{7}$	1	$-20 + 15\langle x\rangle$
38	(3657, 457, 57)	20	2, 5	53	$a^{26} \equiv -1 \pmod{53}$ $a = 2, 5$	1	$-20 + 9\langle x\rangle$
39	(194923, 442, 1)	21	3, 7	463	$a \equiv -1 \pmod{463}$ $a = 3^{231}, 7^{77}$	1	$-21 + \langle x\rangle$
40	(28609, 448, 7)	21	3, 7	67	$a \equiv -1 \pmod{67}$ $a = 3^{11}, 7^{33}$	1	$-21 + 7\langle x\rangle$
41*	(18533, 452, 11)	21	3, 7	43	$a \equiv -1 \pmod{43}$ $a = 3^{21}, 7^{3}$	2	$-21 + 11\langle x\rangle$
42*	(13833, 456, 15)	21	3, 7	53	$a \equiv -1 \pmod{53}$ $a = 3^{26}, 7^{13}$	2	$-21 + 9\langle x\rangle$
43	(4891, 490, 49)	21	3, 7	73	$a \equiv -1 \pmod{73}$ $a = 3^{6}, 7^{12}$	1	$-21 + 7\langle x\rangle$
44	(3649, 513, 72)	21	3, 7	89	$a^{44} \equiv -1 \pmod{89}$ $a = 3, 7$	1	$-21 + 6\langle x\rangle$
45	(2941, 540, 99)	21	3, 7	173	$a^{86} \equiv -1 \pmod{173}$ $a = 3, 7$	1	$21 + 3\langle x\rangle$
46	(1919, 686, 245)	21	3, 7	101	$a^{50} \equiv -1 \pmod{101}$ $a = 3, 7$	1	$-21 + 7\langle x\rangle$
47	(1769, 833, 392)	21	3, 7	61	$a \equiv -1 \pmod{61}$ $a = 3^{5}, 7^{30}$	1	$-21 + 14\langle x\rangle$
48*	(78895, 487, 3)	22	2, 11	509	$a \equiv -1 \pmod{509}$ $a = 2^{254}, 11^{127}$	2	$-22 + \langle x\rangle$
49	(20461, 496, 12)	22	2, 11	37	$a \equiv -1 \pmod{37}$ $a = 2^{18}, 11^{3}$	1	$-22 + 14\langle x\rangle$
50	(4081, 561, 77)	22	2, 11	53	$a \equiv -1 \pmod{53}$ $a = 2^{26}, 11^{13}$	1	$-22 + 11\langle x\rangle$
51	(3835, 568, 84)	22	2, 11	59	$a^{29} \equiv -1 \pmod{59}$ $a = 2, 11$	1	$-22 + 10\langle x\rangle$
52	(3601, 576, 92)	22	2, 11	277	$a \equiv -1 \pmod{277}$ $a = 2^{46}, 11^{138}$	1	$22 + 2\langle x\rangle$
53	(94165, 532, 3)	23	23	37	$23^{6} \equiv -1 \pmod{37}$	1	$-23 + 15\langle x\rangle$
54*	(18531, 545, 16)	23	23	71	$23^{7} \equiv -1 \pmod{71}$	2	$-23 + 8\langle x\rangle$

Table 1: Continued.

	(v, k, λ)	m	p	$\lvert G/N\rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert G/N\rvert}]$	No. of groups of order v	Solutions in G/N
55	(8557, 621, 45)	24	2, 3	43	$a \equiv -1 \pmod{43}$ $a = 2^7, 3^{21}$	1	$-24 + 15\langle x\rangle$
56	(2959, 783, 207)	24	2, 3	269	$a^{134} \equiv -1 \pmod{269}$ $a = 2, 3$	1	$-24 + 3\langle x\rangle$
57*	(131253, 628, 3)	25	5	653	$5^{326} \equiv -1 \pmod{653}$	2	$-25 + \langle x\rangle$
58	(11289, 664, 39)	25	5	53	$5^{26} \equiv -1 \pmod{53}$	1	$-25 + 13\langle x\rangle$
59	(6205, 705, 80)	25	5	73	$5^{36} \equiv -1 \pmod{73}$	1	$-25 + 10\langle x\rangle$
60	(3115, 865, 240)	25	5	89	$5^{22} \equiv -1 \pmod{89}$	1	$-25 + 10\langle x\rangle$

2.4. Amalgamation of Results

In this paper, we study (v, k, λ) difference sets in which $n = k - \lambda = m^2$ and the ideal generated by m factors trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$. That is, if $n = m^2$, then $(n) = (m)(m)$ up to units in $\mathbb{Z}[\zeta_{m'}]$. This method is very useful in the investigation of difference sets in solvable groups. A group G is solvable if the sequence $G \supseteq G' \supseteq G'' \cdots \supseteq \cdots \supseteq G^{(i)} \cdots$ terminates in the identity, $G^{(e)} = 1$, in a finite number of steps, each $G^{(i)}$ is the derived group of the preceding one [28]. Consequently, each i, the factor group $G^{(i)}/G^{(i+1)}$ is Abelian. We now state the extended Sylow theorem in solvable groups ([28], page 141).

Theorem 2.7. *Let G be a solvable group of order mn, in which* $\gcd(m, n) = 1$. *Then*

(1) *G possesses at least one subgroup of order m;*

(2) *any two subgroups of order m are conjugates;*

(3) *any subgroup whose order m' divides m is contained in a subgroup of order m;*

(4) *the number n_m of subgroups of order m may be expressed as a product of factors, each of which (a) is congruent to 1 modulo some prime factor of m, and (b) is a power of a prime and divides one of the chief factors of G.*

The next three criteria enable us to rule out the existence of difference sets.

Criterion 1. Suppose that G is a group of order $v = p's$, where p' is prime, s and t are integers. Then G does not admit (v, k, λ) if there exists a normal subgroup N of G such that

(1) $k - \lambda = m^2$, m is a natural number,

(2) $\lvert G/N\rvert = p'$,

(3) m factors trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{p'}]$, where $\zeta_{p'}$ is the p'th root of unity,

(4) the difference set solution in G/N is one of the forms $\alpha(G/N) + m$, $\alpha + m > \lvert N\rvert$ or $\alpha(G/N) - m$, $\alpha < m$.

Table 2: Partial results in groups of order v by Criterion 1. $C_{|G/N|} = \langle x \rangle$ and parameters with asterisk indicate new results. ? means the number of groups of order v is unknown.

	(v, k, λ)	m	p	$\lvert G/N \rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert G/N \rvert}]$	No. of groups of order v	No. of groups ruled out	Solutions in G/N
1	(171, 51, 15)	6	2,3	19	$a^9 \equiv -1 \pmod{19}$ $a = 2, 3$	5	2	$-6 + 3\langle x \rangle$
2	(155, 56, 20)	6	2,3	31	$3^{15} \equiv -1 \pmod{31}$ 2 factors trivially [20]	2	1	$-6 + 2\langle x \rangle$
3	(231, 70, 21)	7	7	77	$7^5 \equiv -1 \pmod{11}$ 7 factors trivially in $\mathbb{Z}[\zeta_b]$, $b = 11, 77$	2	1	$-7 + 7\langle x \rangle$ in C_7; None in C_{77}
4*	(2325, 84, 3)	9	3	31	$3^{15} \equiv -1 \pmod{31}$	10	3	$-9 + 3\langle x \rangle$,
5*	(10101, 101, 1)	10	2,5	37	$a^{18} \equiv -1 \pmod{37}$ $a = 2, 3$	14	5	$-10 + 3\langle x \rangle$
6	(715, 154, 33)	11	11	143	$11^6 \equiv -1 \pmod{13}$ 11 factors trivially in $\mathbb{Z}[\zeta_b]$, $b = 13, 143$	2	1	$11 + 11\langle x \rangle$ in C_{13}; None in C_{143}
7*	(7155, 147, 3)	12	2,3	53	$a^{26} \equiv -1 \pmod{53}$ $a = 2, 3$	?	?	$-12 + 3\langle x \rangle$
8*	(38613, 197, 1)	14	2,7	211	$a^{105} \equiv -1 \pmod{211}$ $a = 2, 7$	5	2	$-14 + \langle x \rangle$
9*	(5859, 203, 7)	14	2,7	31	$7^{15} \equiv -1 \pmod{31}$ 2 factors trivially [20]	?	?	$-14 + 7\langle x \rangle$
10*	(903, 287, 91)	14	2,7	43	$a \equiv -1 \pmod{43}$ $a = 2^7, 7^3$	7	2	$-14 + 7\langle x \rangle$
11*	(2255, 392, 68)	18	2,3	41	$a \equiv -1 \pmod{41}$ $a = 2^{10}, 3^4$	7	2	$-18 + 10\langle x \rangle$
12*	(160401, 401, 1)	20	2,5	421	$a \equiv -1 \pmod{421}$ $a = 2^{210}, 5^{105}$	5	2	$-20 + \langle x \rangle$
13*	(23607, 407, 7)	20	2,5	61	$a \equiv -1 \pmod{61}$ $a = 2^{30}, 5^{15}$	11	5	$-20 + 7\langle x \rangle$
14*	(22451, 450, 9)	21	3,7	157	$a \equiv -1 \pmod{157}$ $a = 3^{39}, 7^{26}$	2	1	$-21 + 3\langle x \rangle$
15*	(2619, 561, 120)	21	3,7	97	$a \equiv -1 \pmod{97}$ $a = 3^{24}, 7^{48}$	13	5	$-21 + 6\langle x \rangle$
16	(2211, 715, 231)	22	2,11	67	$a^{33} \equiv -1 \pmod{67}$ $a = 2, 11$	4	1	$-22 + 11\langle x \rangle$
17	(7450, 573, 44)	23	23	149	$23^{74} \equiv -1 \pmod{149}$	10	5	$-23 + 4\langle x \rangle$
18	(111555, 579, 3)	24	2,3	67	$a \equiv -1 \pmod{67}$ $a = 2^{33}, 3^{11}$	?	?	$-24 + 9\langle x \rangle$
19	(37961, 585, 9)	24	2,3	29	$a^{14} \equiv -1 \pmod{29}$ $a = 2, 3$	2	1	$-24 + 21\langle x \rangle$
20	(23247, 591, 15)	24	2,3	41	$a \equiv -1 \pmod{41}$ $a = 2^{10}, 3^4$	?	?	$-24 + 15\langle x \rangle$
21	(25641, 641, 16)	25	5	37	$5^{18} \equiv -1 \pmod{37}$	14	4	$-25 + 18\langle x \rangle$

Table 3: Parameter sets that do not exist by Criterion 2. $C_{|H|} = \langle x, y : x^q = y^2 = [x, y]\rangle$ and parameters with asterisk indicate new results. No diff. set image in H implies no difference set image in Dihedral group of same order.

	(v, k, λ)	m	p	$\lvert H\rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert H/\langle g\rangle\rvert}]$	No. of groups of order v	Solutions in H
1	(56, 11, 2)	3	3	14	$3^3 \equiv -1 \pmod 7$	13	$-3 + 2\langle x\rangle$ in $H/\langle g\rangle$
2	(154, 18, 2)	4	2	22	$2^5 \equiv -1 \pmod{11}$	4	$-4 + 2\langle x\rangle$ in $H/\langle g\rangle$
3	(66, 26, 10)	4	2	22	$2^5 \equiv -1 \pmod{11}$	2	$4 + \langle x\rangle\langle y\rangle$; $\langle x\rangle\langle y\rangle + 2(1 + x + y - xy)$
4	(112, 37, 2)	5	5	14	$5^3 \equiv -1 \pmod 7$	43	$-5 + 3\langle x\rangle\langle y\rangle$
5*	(690, 53, 4)	7	7	10	$7^2 \equiv -1 \pmod 5$	8	$-7 + 6\langle x\rangle\langle y\rangle$
6	(496, 55, 6)	7	7	62	7 factors trivially see [21]	42	$-7 + 2\langle x\rangle$ in $H/\langle g\rangle$
7*	(306, 61, 12)	7	7	34	$7^8 \equiv -1 \pmod{17}$	10	$-7 + 4\langle x\rangle$ in $H/\langle g\rangle$
8*	(2146, 66, 2)	8	2	74	$2^{18} \equiv -1 \pmod{37}$	4	$-8 + 2\langle x\rangle$ in $H/\langle g\rangle$
9*	(806, 70, 6)	8	2	26	$2^6 \equiv -1 \pmod{13}$	4	$-8 + 6\langle x\rangle$ in $H/\langle g\rangle$
10*	(430, 78, 14)	8	2	86	$2^7 \equiv -1 \pmod{43}$	4	$-8 + 2\langle x\rangle$ in $H/\langle g\rangle$
11*	(370, 82, 18)	8	2	74	$2^{18} \equiv -1 \pmod{37}$	4	$8 + \langle x\rangle\langle y\rangle$; $\langle x\rangle\langle y\rangle + 4(1 + x + y - xy)$
12*	(266, 106, 42)	8	2	38	$2^9 \equiv -1 \pmod{19}$	4	$-8 + 6\langle x\rangle$ in $H/\langle g\rangle$
13*	(3404, 83, 2)	9	3	46	Remark 2.3	11	$-9 + 4\langle x\rangle$ in $H/\langle g\rangle$
14*	(714, 93, 12)	9	3	34	$3^8 \equiv -1 \pmod{17}$	12	$-9 + 6\langle x\rangle$ in $H/\langle g\rangle$
15*	(2668, 127, 6)	11	11	46	Remark 2.3	11	$-11 + 6\langle x\rangle$ in $H/\langle g\rangle$
16*	(1704, 131, 10)	11	11	142	$11^{35} \equiv -1 \pmod{71}$	39	$-11 + 2\langle x\rangle$ in $H/\langle g\rangle$
17*	(1450, 162, 18)	12	2,3	58	$a^{14} \equiv -1 \pmod{29}$ $a = 2, 3$	10	$-12 + 6\langle x\rangle$ in $H/\langle g\rangle$
18*	(760, 253, 84)	13	13	38	$13^9 \equiv -1 \pmod{19}$	39	$-13 + 7\langle x\rangle\langle y\rangle$
19*	(13054, 229, 4)	15	3,5	122	$a^5 \equiv -1 \pmod{61}$ $a = 3, 5$	4	$-15 + 4\langle x\rangle$ in $H/\langle g\rangle$
20*	(4064, 239, 14)	15	3, 5	254	$a \equiv -1 \pmod{127}$ $a = 3^{63}, 5^{21}$	195	$-15 + 2\langle x\rangle$ in $H/\langle g\rangle$
21*	(3268, 243, 18)	15	3,5	86	$a^{21} \equiv -1 \pmod{43}$ $a = 3, 5$	9	$-15 + 6\langle x\rangle$ in $H/\langle g\rangle$
22*	(2278, 253, 28)	15	3,5	134	$a^{11} \equiv -1 \pmod{67}$ $a = 3, 5$	4	$-15 + 4\langle x\rangle$ in $H/\langle g\rangle$
23*	(1886, 261, 36)	15	3,5	46	Remark 2.3	4	$-15 + 12\langle x\rangle$ in $H/\langle g\rangle$

Table 3: Continued.

	(v, k, λ)	m	p	$\lvert H\rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert H/\langle g\rangle\rvert}]$	No. of groups of order v	Solutions in H
24*	(1406, 281, 56)	15	3,5	74	$a \equiv -1 \pmod{37}$ $a = 3^9, 5^{18}$	4	$-15 + 8\langle x\rangle$ in $H/\langle g\rangle$
25*	(1054, 325, 100)	15	3,5	34	$a^8 \equiv -1 \pmod{17}$ $a = 3, 5$	4	$-15 + 10\langle x\rangle\langle y\rangle$
26*	(918, 393, 168)	15	3,5	34	$a^8 \equiv -1 \pmod{17}$ $a = 3, 5$	30	$-15 + 12\langle x\rangle\langle y\rangle$
27*	(902, 425, 200)	15	3,5	82	$a \equiv -1 \pmod{41}$ $a = 3^4, 5^{10}$	4	$15 + 5\langle x\rangle\langle y\rangle$
28*	(33154, 258, 2)	16	2	274	$2^{34} \equiv -1 \pmod{137}$	10	$-16 + 2\langle x\rangle$ in $H/\langle g\rangle$
29*	(11398, 262, 6)	16	2	278	$2^{69} \equiv -1 \pmod{139}$	4	$-16 + 2\langle x\rangle$ in $H/\langle g\rangle$
30*	(2466, 290, 34)	16	2	274	$2^{34} \equiv -1 \pmod{137}$	10	$16 + \langle x\rangle\langle y\rangle$; $\langle x\rangle\langle y\rangle + 8(1 + x + y - xy)$
31*	(1660, 316, 60)	16	2	166	$2^{41} \equiv -1 \pmod{83}$	11	$-16 + 4\langle x\rangle$ in $H/\langle g\rangle$
32*	(1066, 426, 170)	16	2	82	$2^{10} \equiv -1 \pmod{41}$	4	$16 + 5\langle x\rangle\langle y\rangle$; $5\langle x\rangle\langle y\rangle + 8(1 + x + y - xy)$
33*	(7526, 301, 12)	17	17	106	$17^{13} \equiv -1 \pmod{53}$	4	$-17 + 6\langle x\rangle$ in $H/\langle g\rangle$
34*	(5796, 305, 16)	17	17	46	$17^{11} \equiv -1 \pmod{23}$	111	$-17 + 14\langle x\rangle$ in $H/\langle g\rangle$
35*	(20758, 408, 8)	20	2,5	214	$a^{53} \equiv -1 \pmod{107}$ $a = 2, 5$	4	$-20 + 4\langle x\rangle$ in $H/\langle g\rangle$
36*	(7474, 424, 24)	20	2,5	74	$a^{18} \equiv -1 \pmod{37}$ $a = 2, 5$	4	$-20 + 12\langle x\rangle$ in $H/\langle g\rangle$
37*	(5038, 438, 38)	20	2,5	458	$a \equiv -1 \pmod{229}$ $a = 2^{38}, 5^{57}$	4	$-20 + 2\langle x\rangle$ in $H/\langle g\rangle$
38*	(2014, 550, 150)	20	2,5	106	$a^{26} \equiv -1 \pmod{53}$ $a = 2, 5$	4	$20 + 5\langle x\rangle\langle y\rangle$; $5\langle x\rangle\langle y\rangle + 10(1+x+y-xy)$
39*	(1918, 568, 168)	20	2,5	274	$a \equiv -1 \pmod{137}$ $a = 2^{34}, 5^{68}$	4	$20 + 4\langle x\rangle$ in $H/\langle g\rangle$
40*	(24346, 541, 12)	23	23	94	$23^{23} \equiv -1 \pmod{47}$	8	$-23 + 12\langle x\rangle$ in $H/\langle g\rangle$
41*	(34282, 586, 10)	24	2, 3	122	$a \equiv -1 \pmod{61}$ $a = 2^{30}, 3^5$	4	$-24 + 10\langle x\rangle$ in $H/\langle g\rangle$
42*	(20770, 645, 20)	25	5	134	$5^{11} \equiv -1 \pmod{67}$	12	$-25 + 10\langle x\rangle$ in $H/\langle g\rangle$

Proof. The nonexistence of viable difference set image in G/N implies that G does not admit (v, k, λ) difference set. □

In this criterion, we may replace $|G/N| = p'$ with $|G/N| = p'q$ if $q > 2$ is prime power, $q \mid s$, $\gcd(p', q) = 1$, and the ideal generated by p factors trivially in $\mathbb{Z}[\zeta_{p'q}]$, where p is a prime divisor of m (see Remark 2.3).

Table 4: Partial results in groups of order v by Criterion 2. $C_{|H|} = \langle x, y : x^q = y^2 = [x, y]\rangle$ and parameters with asterisk indicate new results. No difference set image in H implies no diff. set image in Dihedral group of same order. ? means the number of groups of order v is unknown.

	(v, k, λ)	m	p	$\lvert H\rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert H/\langle g\rangle\rvert}]$	No. of groups of order v	No. of groups ruled out	Solutions in H
1	(78, 22, 6)	4	2	26	$2^6 \equiv -1 \pmod{13}$	6	4	$-4 + 2\langle x\rangle$ in $H/\langle g\rangle$
2	(204, 29, 4)	5	5	34	$5^8 \equiv -1 \pmod{17}$	12	10	$-5 + 2\langle x\rangle$ in $H/\langle g\rangle$
3*	(1140, 68, 4)	8	2	38	$2^9 \equiv -1 \pmod{19}$	41	29	$-8 + 4\langle x\rangle$ in $H/\langle g\rangle$
4*	(396, 80, 16)	8	2	66	$2^5 \equiv -1 \pmod{b}$ $b = 11, 33$	30	15	None in $H/\langle g\rangle$
5*	(300, 92, 48)	8	2	50	$2^{10} \equiv -1 \pmod{25}$	49	9	$-8 + 4\langle x\rangle$ in $H/\langle g\rangle$
6*	(980, 89, 8)	9	3	14	$3^3 \equiv -1 \pmod{7}$	34	31	$-9 + 7\langle x\rangle\langle y\rangle$
7*	(456, 105, 24)	9	3	38	$3^9 \equiv -1 \pmod{19}$	54	39	$-9 + 6\langle x\rangle$ in $H/\langle g\rangle$
8*	(1856, 106, 6)	10	2, 5	58	$a \equiv -1 \pmod{29}$ $a = 2^{14}, 5^7$	1630	1387	$-10 + 4\langle x\rangle$ in $H/\langle g\rangle$
9*	(7504, 123, 2)	11	11	134	$11^{33} \equiv -1 \pmod{67}$	?	?	$-11 + 2\langle x\rangle$ in $H/\langle g\rangle$
10*	(3876, 125, 4)	11	11	34	$11^8 \equiv -1 \pmod{17}$	40	34	$-11 + 8\langle x\rangle$ in $H/\langle g\rangle$
11*	(2870, 152, 8)	12	2, 3	82	$a \equiv -1 \pmod{41}$ $a = 2^{10}, 3^4$	12	8	$-12 + 4\langle x\rangle$ in $H/\langle g\rangle$
12*	(666, 210, 66)	12	2, 3	74	$a \equiv -1 \pmod{37}$ $a = 2^{18}, 3^9$	18	10	$-12 + 6\langle x\rangle$ in $H/\langle g\rangle$
13*	(610, 232, 88)	12	2, 3	122	$a \equiv -1 \pmod{61}$ $a = 2^{30}, 3^5$	6	4	$-12 + 4\langle x\rangle$ in $H/\langle g\rangle$
14*	(14536, 171, 2)	13	13	46	Remark 2.3	?	?	$-13 + 8\langle x\rangle$ in $H/\langle g\rangle$
15*	(7440, 173, 4)	13	13	62	$13^{15} \equiv -1 \pmod{31}$	?	?	$-13 + 6\langle x\rangle$ in $H/\langle g\rangle$
16*	(5076, 175, 6)	13	13	94	$13^{23} \equiv -1 \pmod{47}$	?	?	$-13 + 4\langle x\rangle$ in $H/\langle g\rangle$
17*	(2716, 181, 12)	13	13	194	$13^{48} \equiv -1 \pmod{97}$	11	9	$-13 + 2\langle x\rangle$ in $H/\langle g\rangle$
18*	(19504, 198, 2)	14	2, 7	106	$a \equiv -1 \pmod{53}$ $a = 2^{26}, 7^{13}$	?	?	$-14 + 4\langle x\rangle$ in $H/\langle g\rangle$
19*	(1696, 226, 30)	14	2, 7	212	$2^{26} \equiv -1 \pmod{53}$ $7^{13} \equiv -1 \pmod{b}$ $b = 53, 106, 212$	235	194	$14 + \langle x\rangle\langle y\rangle$
20*	(8856, 231, 6)	15	3, 5	82	$a \equiv -1 \pmod{41}$ $a = 3^4, 5^{20}$	?	?	$-15 + 6\langle x\rangle$ in $H/\langle g\rangle$
21*	(1508, 275, 50)	15	3, 5	58	$a \equiv -1 \pmod{29}$ $a = 3^{14}, 5^7$	15	11	$-15 + 10\langle x\rangle$ in $H/\langle g\rangle$
22*	(976, 351, 126)	15	3, 5	122	$a \equiv -1 \pmod{61}$ $a = 3^5, 5^{15}$	51	14	$-15 + 6\langle x\rangle$ in $H/\langle g\rangle$
23*	(3256, 280, 24)	16	2	74	$2^{18} \equiv -1 \pmod{37}$	?	?	$-16 + 8\langle x\rangle$ in $H/\langle g\rangle$

Table 4: Continued.

	(v, k, λ)	m	p	$\lvert H\rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert H/\langle g\rangle\rvert}]$	No. of groups of order v	No. of groups ruled out	Solutions in H
24*	(1036, 460, 204)	16	2	74	$2^{18} \equiv -1 \pmod{37}$	11	9	$16 + 6\langle x\rangle\langle y\rangle$; $6\langle x\rangle\langle y\rangle + 8(1 + x + y - xy)$
25*	(21390, 293, 4)	17	17	62	$17^{15} \equiv -1 \pmod{31}$	36	16	$-17 + 10\langle x\rangle$ in $H/\langle g\rangle$
26*	(52976, 326, 2)	18	2, 3	86	$3^{21} \equiv -1 \pmod{43}$ See Remark 2.2 for $\langle 2\rangle$	?	?	$-18 + 8\langle x\rangle$ in $H/\langle g\rangle$
27*	(18096, 330, 6)	18	2, 3	58	$a^{14} \equiv -1 \pmod{29}$ $a = 2, 3$	?	?	$-18 + 12\langle x\rangle$ in $H/\langle g\rangle$
28*	(1776, 426, 102)	18	2, 3	74	$a \equiv -1 \pmod{37}$ $a = 2^{18}, 3^{9}$	260	170	$-18 + 12\langle x\rangle$ in $H/\langle g\rangle$
29*	(65704, 363, 2)	19	19	382	$19^{95} \equiv -1 \pmod{191}$	?	?	$-19 + 2\langle x\rangle$ in $H/\langle g\rangle$
30*	(22388, 367, 6)	19	19	386	$19^{96} \equiv -1 \pmod{193}$	15	11	$-19 + 2\langle x\rangle$ in $H/\langle g\rangle$
31*	(13728, 371, 10)	19	19	26	$19^{6} \equiv -1 \pmod{13}$	?	?	$-19 + 15\langle x\rangle\langle y\rangle$
32*	(7960, 379, 18)	19	19	398	$19^{9} \equiv -1 \pmod{199}$	?	?	$-19 + 2\langle x\rangle$ in $H/\langle g\rangle$
33*	(5084, 391, 30)	19	19	82	$19^{20} \equiv -1 \pmod{41}$	11	9	$-19 + 10\langle x\rangle$ in $H/\langle g\rangle$
34*	(2256, 451, 90)	19	19	94	$19^{23} \equiv -1 \pmod{47}$	?	?	$-19 + 10\langle x\rangle$ in $H/\langle g\rangle$
35*	(40704, 404, 4)	20	2, 5	106	$a^{26} \equiv -1 \pmod{53}$ $a = 2, 5$	?	?	$-20 + 8\langle x\rangle$ in $H/\langle g\rangle$
36*	(16770, 410, 10)	20	2, 5	86	$a \equiv -1 \pmod{43}$ $a = 2^{7}, 5^{21}$	48	24	$-20 + 10\langle x\rangle$ in $H/\langle g\rangle$
37*	(1830, 590, 190)	20	2, 5	122	$a \equiv -1 \pmod{61}$ $a = 2^{30}, 5^{15}$	18	8	$-20 + 10\langle x\rangle$in $H/\langle g\rangle$
38*	(49369, 445, 4)	21	3, 7	466	$a \equiv -1 \pmod{233}$ $a = 3^{116}, 7^{58}$	15	11	$-21 + 2\langle x\rangle$ in $H/\langle g\rangle$
39*	(17064, 453, 12)	21	3, 7	158	$a^{39} \equiv -1 \pmod{79}$ $a = 3, 7$	?	?	$-21 + 6\langle x\rangle$ in $H/\langle g\rangle$
40*	(14756, 455, 14)	21	3, 7	34	$a^{8} \equiv -1 \pmod{17}$ $a = 3, 7$	27	23	$-21 + 14\langle x\rangle\langle y\rangle$
41*	(10604, 461, 20)	21	3, 7	482	$a \equiv -1 \pmod{241}$ $a = 3^{60}, 7^{120}$	11	9	$-21 + 2\langle x\rangle$ in $H/\langle g\rangle$
42*	(7380, 471, 30)	21	3, 7	82	$a \equiv -1 \pmod{41}$ $a = 3^{4}, 7^{20}$	149	89	$-21 + 12\langle x\rangle$ in $H/\langle g\rangle$
43*	(5336, 485, 44)	21	3, 7	46	Remark 2.3	?	?	$-21 + 11\langle x\rangle\langle y\rangle$
44*	(3128, 531, 90)	21	3, 7	46	Remark 2.3	?	?	$-21 + 12\langle x\rangle\langle y\rangle$
45*	(2408, 581, 140)	21	3, 7	86	$a \equiv -1 \pmod{43}$ $a = 3^{21}, 7^{3}$	?	?	$-21 + 14\langle x\rangle$ in $H/\langle g\rangle$
46*	(70890, 533, 4)	23	23	278	$23^{23} \equiv -1 \pmod{139}$	24	16	$-23 + 4\langle x\rangle$ in $H/\langle g\rangle$
47*	(47616, 535, 8)	23	23	62	$23^{5} \equiv -1 \pmod{31}$	?	?	$-23 + 18\langle x\rangle$ in $H/\langle g\rangle$
48*	(13776, 551, 22)	23	23	82	$23^{5} \equiv -1 \pmod{41}$	?	?	$-23 + 7\langle x\rangle\langle y\rangle$

Table 4: Continued.

	(v, k, λ)	m	p	$\lvert H\rvert$	Factoring of p in $\mathbb{Z}[\zeta_{\lvert H/\langle g\rangle\rvert}]$	No. of groups of order v	No. of groups ruled out	Solutions in H
49*	(166754, 578, 2)	24	2, 3	86	$a \equiv -1 \pmod{43}$ $a = 2^7, 3^{21}$	12	8	$-24 + 14\langle x\rangle$ in $H/\langle g\rangle$
50*	(56358, 582, 6)	24	2, 3	202	$a^{50} \equiv -1 \pmod{101}$ $a = 2, 3$	?	?	$-24 + 6\langle x\rangle$ in $H/\langle g\rangle$
51*	(10388, 612, 36)	24	2, 3	106	$a^{26} \equiv -1 \pmod{53}$ $a = 2, 3$	34	28	$-24 + 12\langle x\rangle$ in $H/\langle g\rangle$
52*	(4844, 668, 92)	24	2, 3	346	$a^{86} \equiv -1 \pmod{173}$ $a = 2, 3$	11	9	$-24 + 4\langle x\rangle$ in $H/\langle g\rangle$
53*	(3690, 714, 138)	24	2, 3	82	$a \equiv -1 \pmod{41}$ $a = 2^{10}, 3^4$	30	20	$-24 + 18\langle x\rangle$ in $H/\langle g\rangle$
54*	(3172, 756, 180)	24	2, 3	122	$a \equiv -1 \pmod{61}$ $a = 2^{30}, 3^5$	15	11	$24 + 6\langle x\rangle\langle y\rangle$, $6\langle x\rangle\langle y\rangle + 12(1 + x + y - xy)$
55*	(2332, 1036, 460)	24	2, 3	106	$a^{26} \equiv -1 \pmod{53}$ $a = 2, 3$	11	9	$-24 + 20\langle x\rangle$ in $H/\langle g\rangle$
56*	(196252, 627, 2)	25	5	326	$5^{27} \equiv -1 \pmod{163}$	?	?	$-25 + 4\langle x\rangle$ in $H/\langle g\rangle$
57*	(66256, 631, 6)	25	5	82	$5^{10} \equiv -1 \pmod{41}$	?	?	$-25 + 16\langle x\rangle$ in $H/\langle g\rangle$
58*	(50008, 633, 8)	25	5	94	$5^{23} \equiv -1 \pmod{47}$	?	?	$-25 + 14\langle x\rangle$ in $H/\langle g\rangle$
59*	(17524, 649, 24)	25	5	674	$5^{56} \equiv -1 \pmod{337}$	15	11	$-25 + 2\langle x\rangle\langle y\rangle$
60*	(14280, 655, 30)	25	5	34	$5^8 \equiv -1 \pmod{17}$	?	?	$-25 + 20\langle x\rangle\langle y\rangle$
61*	(11040, 665, 40)	25	5	12	$5 \equiv -1 \pmod{b}$ $b = 2, 3$	?	?	$-25 + 115\langle x\rangle$ in $H/\langle g\rangle$
62*	(11040, 665, 40)	25	5	46	Remark 2.3	?	?	$-25 + 15\langle x\rangle\langle y\rangle$
63*	(5104, 729, 104)	25	5	58	$5^7 \equiv -1 \pmod{29}$	?	?	$-25 + 13\langle x\rangle\langle y\rangle$
64*	(2812, 937, 312)	25	5	74	$5^{18} \equiv -1 \pmod{37}$	11	9	$-25 + 13\langle x\rangle\langle y\rangle$

Criterion 2. Suppose that G is a group of even order v and H is a factor group of G with $|H| = 2q$, where q is prime. Let g be an element of order 2 in H. Then G does not admit (v, k, λ) if

(1) $k - \lambda = m^2$, m is a natural number,

(2) m factors trivially in the cyclotomic rings $\mathbb{Z}[\zeta_q]$, where ζ_q is qth root of unity,

(3) the difference set solution in $H/\langle g\rangle$ is one of the forms $\alpha(H/\langle g\rangle) + m$, $\alpha + m > |G/(H/\langle g\rangle)|$ or $\alpha(H/\langle g\rangle) - m$, $\alpha < m$; alternatively, the difference set image in H is one of the forms $\alpha(H) + m$, $\alpha + m > |G/H|$ or $\alpha(H) - m$, $\alpha < m$.

Proof. The proof follows from Criterion 1 and the fact that if $|H| \equiv 2 \pmod 4$, the cyclotomic rings $\mathbb{Z}[\zeta_{2q}]$ and $\mathbb{Z}[\zeta_q]$ are the same. □

Criterion 3. Suppose that G is a group of order $v = 2^2 \times q \times s$, where $q \geq 3$ is prime and s is an integer. Suppose that H is a factor group of G of order $2q$. The group G does not admit (v, k, λ) difference set if there exists a normal subgroup N such that $G/N \cong H \times C_2$ and

(1) $k - \lambda = m^2$, m is a natural number,

(2) every prime divisor m' of m factors trivially in the cyclotomic rings $\mathbb{Z}[\zeta_q]$, where ζ_q is qth root of unity, $\gcd(m', q) = 1$

Table 5: Partial results in groups of order v by Criterion 3. Parameters with asterisk indicate new results.? means the number of groups of order v is unknown.

	(v, k, λ)	m	p	Factoring of p in $\mathbb{Z}[\zeta_q]$	No. of groups of order v	No. of groups ruled out	Solutions in H
1	(40, 13, 4)	3	3	$3^2 \equiv -1 \pmod{b}$ $b = 5, 10$	14	10	$3 + H$, $\lvert H\rvert = 10$
2*	(400, 57, 8)	7	7	$7^2 \equiv -1 \pmod{b}$ $b = 5, 10$	221	166	$7 + 5H$, $\lvert H\rvert = 10$
3*	(280, 63, 14)	7	7	$7^2 \equiv -1 \pmod{b}$ $b = 5, 10$	40	30	$-7 + 7H$, $\lvert H\rvert = 10$
4*	(220, 73, 24)	7	7	$7^2 \equiv -1 \pmod{b}$ $b = 5, 10$	15	7	$-7 + 8H$, $\lvert H\rvert = 10$
5*	(820, 91, 10)	9	3	$3^2 \equiv -1 \pmod{b}$ $b = 5, 10$	20	7	$-9 + 10H$, $\lvert H\rvert = 10$
6*	(540, 99, 18)	9	3	$3^2 \equiv -1 \pmod{b}$ $b = 5, 10$	119	56	$9 + 9H$, $\lvert H\rvert = 10$
7*	(3876, 125, 4)	11	11	$11 \equiv -1 \pmod{b}$ $b = 3, 6, 12$	40	32	$11 + 19H$, $\lvert H\rvert = 6$
8*	(1464, 133, 12)	11	11	$11^2 \equiv -1 \pmod{61}$	61	30	$11 + H$, $\lvert H\rvert = 122$
9*	(988, 141, 30)	11	11	$11^6 \equiv -1 \pmod{b}$ $b = 13, 26$	11	5	$11 + 5H$, $\lvert H\rvert = 26$
10*	(756, 151, 30)	11	11	$11 \equiv -1 \pmod{b}$ $b = 3, 6, 12$	189	96	$-11 + 27H$, $\lvert H\rvert = 6$
11*	(2380, 183, 14)	13	13	$13^2 \equiv -1 \pmod{17}$	35	15	$13 + 5H$, $\lvert H\rvert = 34$
12*	(1056, 211, 42)	13	13	$13^5 \equiv -1 \pmod{11}$	1028	995	$13 + 9H$, $\lvert H\rvert = 22$
13*	(1456, 195, 26)	13	13	$13 \equiv -1 \pmod{7}$	179	171	$13 + 13H$, $\lvert H\rvert = 14$
14*	(1380, 197, 28)	13	13	$13^2 \equiv -1 \pmod{b}$ $b = 5, 10$	29	15	$-13 + 21H$, $\lvert H\rvert = 10$
15*	(1548, 273, 48)	15	3, 5	$a^{21} \equiv -1 \pmod{43}$ $a = 3, 5$	46	6	$15 + 3H$, $\lvert H\rvert = 86$
16*	(1160, 305, 80)	15	3, 5	$a \equiv -1 \pmod{29}$ $a = 3^{14}, 5^7$	49	33	$15 + 5H$, $\lvert H\rvert = 58$
17*	(1012, 337, 112)	15	3, 5	$5^{11} \equiv -1 \pmod{23}$ Remark 2.3	13	5	$15 + 7H$, $\lvert H\rvert = 46$
18*	(1300, 433, 144)	17	17	$17^2 \equiv -1 \pmod{b}$ $b = 5, 10$	50	16	$-17 + 45H$, $\lvert H\rvert = 10$
19*	(5220, 307, 18)	17	17	$17^2 \equiv -1 \pmod{b}$ $b = 5, 10$	113	50	$17 + 29H$, $\lvert H\rvert = 10$
20*	(5220, 307, 18)	17	17	$17^2 \equiv -1 \pmod{29}$	113	50	$17 + 5H$, $\lvert H\rvert = 58$
21*	(5220, 307, 18)	17	17	$17 \equiv -1 \pmod{b}$ $b = 3, 6$	113	50	$-17 + 27H$, $\lvert H\rvert = 12$
22*	(33216, 365, 4)	19	19	$19^{86} \equiv -1 \pmod{173}$	?	?	$19 + H$, $\lvert H\rvert = 346$
23*	(11564, 373, 12)	19	19	$19^3 \equiv -1 \pmod{7}$	28	16	$-19 + 28H$, $\lvert H\rvert = 14$
24*	(7240, 381, 20)	19	19	$19^2 \equiv -1 \pmod{181}$	?	?	$19 + H$, $\lvert H\rvert = 362$
25*	(4368, 397, 36)	19	19	$19^3 \equiv -1 \pmod{7}$	?	?	$19 + 27H$, $\lvert H\rvert = 14$
26*	(4180, 399, 38)	19	19	$19^5 \equiv -1 \pmod{11}$	36	15	$-19 + 19H$, $\lvert H\rvert = 22$
27*	(2508, 437, 76)	19	19	$19^5 \equiv -1 \pmod{11}$	34	20	$19 + 19H$, $\lvert H\rvert = 22$
28*	(1976, 475, 114)	19	19	$19^6 \equiv -1 \pmod{13}$	39	30	$-19 + 19H$, $\lvert H\rvert = 26$
29*	(1624, 541, 180)	19	19	$19^{14} \equiv -1 \pmod{29}$	56	30	$19 + 9H$, $\lvert H\rvert = 58$

Table 5: Continued.

	(v, k, λ)	m	p	Factoring of p in $\mathbb{Z}[\zeta_q]$	No. of groups of order v	No. of groups ruled out	Solutions in H
30*	(1520, 589, 228)	19	19	$19^3 \equiv -1 \pmod{b}$ $b = 5, 10$	178	147	$19 + 57H$, $\lvert H\rvert = 10$
31*	(97904, 443, 2)	21	3, 7	$a^{105} \equiv -1 \pmod{211}$ $a = 3, 7$	?	?	$21 + H$, $\lvert H\rvert = 422$
32*	(11680, 459, 18)	21	3, 7	$a \equiv -1 \pmod{73}$ $a = 3^6, 7^{12}$	?	?	$21 + 3H$, $\lvert H\rvert = 146$
33*	(9724, 463, 22)	21	3, 7	$a^8 \equiv -1 \pmod{17}$ $a = 3, 7$	35	15	$21 + 13H$, $\lvert H\rvert = 34$
34*	(7840, 469, 28)	21	3, 7	$a^2 \equiv -1 \pmod{5}$ $a = 3, 7$	?	?	$-21 + 49H$, $\lvert H\rvert = 10$
35*	(7380, 471, 30)	21	3, 7	$a^2 \equiv -1 \pmod{5}$ $a = 3, 7$	149	66	$21 + 45H$, $\lvert H\rvert = 10$
36*	(3128, 531, 90)	21	3, 7	$a^8 \equiv -1 \pmod{17}$ $a = 3, 7$	?	?	$21 + 15H$, $\lvert H\rvert = 34$
37*	(2756, 551, 110)	21	3, 7	$a \equiv -1 \pmod{53}$ $a = 3^{26}, 7^{13}$	20	5	$21 + 5H$, $\lvert H\rvert = 106$
38*	(2296, 595, 154)	21	3, 7	$a \equiv -1 \pmod{41}$ $a = 3^4, 7^{20}$	?	?	$21 + 7H$, $\lvert H\rvert = 82$
39*	(1904, 693, 252)	21	3, 7	$a^8 \equiv -1 \pmod{17}$ $a = 3, 7$	186	147	$-21 + 21H$, $\lvert H\rvert = 34$
40*	(1836, 735, 294)	21	3, 7	$a \equiv -1 \pmod{17}$ $a = 3^2, 7^2$	117	56	$21 + 21H$, $\lvert H\rvert = 34$
41*	(1820, 749, 308)	21	3, 7	$a \equiv -1 \pmod{5}$ $a = 3^2, 7^2$	35	15	$-21 + 77H$, $\lvert H\rvert = 10$
42*	(1800, 771, 330)	21	3, 7	$a \equiv -1 \pmod{5}$ $a = 3^2, 7^2$	749	412	$21 + 75H$, $\lvert H\rvert = 10$
43*	(47616, 535, 6)	23	23	$23 \equiv -1 \pmod{3}$	?	?	$-23 + 93H$, $\lvert H\rvert = 6$
44*	(35980, 537, 8)	23	23	$23^{32} \equiv -1 \pmod{257}$	35	15	$23 + H$, $\lvert H\rvert = 514$
45*	(12720, 553, 24)	23	23	$23^2 \equiv -1 \pmod{5}$	?	?	$23 + 53H$, $\lvert H\rvert = 10$
46*	(12720, 553, 24)	23	23	$23^2 \equiv -1 \pmod{53}$	?	?	$23 + 5H$, $\lvert H\rvert = 106$
47*	(7176, 575, 46)	23	23	$23^3 \equiv -1 \pmod{13}$	?	?	$-23 + 23H$, $\lvert H\rvert = 26$
48*	(4320, 617, 88)	23	23	$23 \equiv -1 \pmod{3}$	?	?	$23 + 99H$, $\lvert H\rvert = 6$
49*	(3220, 667, 138)	23	23	$23^2 \equiv -1 \pmod{5}$	27	15	$-23 + 69H$, $\lvert H\rvert = 10$
50*	(2760, 713, 184)	23	23	$23 \equiv -1 \pmod{3}$	?	?	$23 + 115H$, $\lvert H\rvert = 6$
51*	(2760, 713, 184)	23	23	$23^2 \equiv -1 \pmod{5}$	?	?	$23 + 69H$, $\lvert H\rvert = 10$
52*	(2380, 793, 264)	23	23	$23^8 \equiv -1 \pmod{17}$	35	15	$-23 + 24H$, $\lvert H\rvert = 34$
53*	(2380, 793, 264)	23	23	$23^2 \equiv -1 \pmod{5}$	35	15	$23 + 77H$, $\lvert H\rvert = 10$
54*	(196252, 627, 2)	25	5	$5^3 \equiv -1 \pmod{7}$	?	?	$25 + 43H$, $\lvert H\rvert = 14$
55*	(196252, 627, 2)	25	5	$5^{21} \equiv -1 \pmod{43}$	?	?	$25 + 7H$, $\lvert H\rvert = 86$
56*	(40260, 635, 10)	25	5	$5^{15} \equiv -1 \pmod{61}$	370	66	$25 + 5H$, $\lvert H\rvert = 122$
57*	(16276, 651, 26)	25	5	$5^4 \equiv -1 \pmod{313}$	20	5	$25 + H$, $\lvert H\rvert = 626$
58*	(14280, 655, 30)	25	5	$5^3 \equiv -1 \pmod{7}$	?	?	$25 + 45H$, $\lvert H\rvert = 14$
59*	(11040, 665, 40)	25	5	$5 \equiv -1 \pmod{3}$	?	?	$-25 + 115H$, $\lvert H\rvert = 6$
60*	(9100, 675, 50)	25	5	$5^2 \equiv -1 \pmod{13}$	118	50	$25 + 25H$, $\lvert H\rvert = 26$

Table 5: Continued.

	(v, k, λ)	m	p	Factoring of p in $\mathbb{Z}[\zeta_q]$	No. of groups of order v	No. of groups ruled out	Solutions in H
61*	(6328, 703, 78)	25	5	$5^{56} \equiv -1 \pmod{113}$	?	?	$25 + 3H$, $\lvert H\rvert = 226$
62*	(4620, 745, 120)	25	5	$5^3 \equiv -1 \pmod 7$	140	66	$-25 + 55H$, $\lvert H\rvert = 14$
63*	(4380, 755, 130)	25	5	$5^{36} \equiv -1 \pmod{73}$	53	15	$25 + 5H$, $\lvert H\rvert = 146$
64*	(3400, 825, 200)	25	5	$5^8 \equiv -1 \pmod{17}$	?	?	$-25 + 25H$, $\lvert H\rvert = 34$
65*	(3060, 875, 250)	25	5	$5^8 \equiv -1 \pmod{17}$	113	50	$25 + 25H$, $\lvert H\rvert = 34$
66*	(2640, 1015, 390)	25	5	$5 \equiv -1 \pmod 3$	?	?	$25 + 165H$, $\lvert H\rvert = 6$
67*	(2520, 1145, 520)	25	5	$5 \equiv -1 \pmod 3$	?	?	$-25 + 195H$, $\lvert H\rvert = 6$

(3) the difference set solution in H is of the form $\alpha H + m$, and α is an odd integer or

(4) the difference set solution in H is of the form $\alpha H - m$, α is an even integer, m is an odd integer, and $m > \alpha/2$.

Proof. There are two groups of order $2q$, cyclic and dihedral groups. Since every prime divisor m' of m factors trivially in the cyclotomic rings $\mathbb{Z}[\zeta_q]$, $\gcd(m', q) = 1$, it follows that m factors trivially in $\mathbb{Z}[\zeta_q]$. Consequently, the (v, k, λ) difference set image in H is of the form $\alpha H + m$ or $\alpha H - m$. Suppose that the (v, k, λ) difference set image in H is of the form $\alpha H + m$ and α is an odd integer. Using (2.8), the difference set image in $H \times C_2$ is

$$\widehat{D} = A\left(\frac{\langle z\rangle}{2}\right) + gB\left(\frac{2 - \langle z\rangle}{2}\right), \tag{2.9}$$

where $g \in H \times C_2$, $A = \alpha H + m$ is the difference set image in H, $B = A - \alpha H$ with $\alpha = (k+m)/2q$ or $(k - m)/2q$ and z is the generator of C_2. Since α is odd, $A(\langle z\rangle/2)$ consists of at least $2q - 2$ odd entries while $B((2 - \langle z\rangle)/2)$ consists of at least $2q - 2$ even entries. Thus, (2.8) has no integer solutions. On the other hand, suppose that the (v, k, λ) difference set image in H is of the form $\alpha H - m$, α is an even integer, m is odd an odd integer, and $m > \alpha/2$. The difference set image is of the form (2.9) with $A = \alpha H - m$. Since α is even and m is odd, $A(\langle z\rangle/2)$ and $B((2 - \langle z\rangle)/2)$ have two entries that are fractions. In particular, we can translate if necessary, to ensure that the coefficients of the identity in both components are $(\alpha - m)/2$ and $-m/2$, respectively. The sum and difference of these two entries are, respectively, $(\alpha - 2m)/2$ and $\alpha/2$. But $m > \alpha/2$ and $2m > \alpha$. Hence, $(\alpha - 2m)/2$ is a negative integer. Thus, there is no difference set image in $H \times C_2$ and the criterion follows. □

Notice that there are five factor groups of order $2^2 \times q$ if $q \equiv 1 \pmod 4$ and four factor groups if $q \equiv 3 \pmod 4$. Criterion 3 rules out the existence of difference set images in $C_q \times C_2 \times C_2$ and $D_{2q} \cong D_q \times C_2$. In addition to conditions of Criterion 3, if m factors trivially also in $\mathbb{Z}[\zeta_{2^2 \times q}]$, then three of the four or five factor groups (C_{2q}, $C_q \times C_2 \times C_2$ and D_{2q}) of order $2^2 \times q$ do not admit difference sets.

3. Some Difference Sets Parameters (Tables 1–5)

We list some parameter sets (both known and new) that do not exist. In each of these cases, G is a group of order v and $\varphi : G \to H$ is a group homomorphism. Suppose that D is a k-subset of G and $n = k - \lambda = m^2$ such that m factors trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{|H|}]$. We use Criteria 1, 2 and 3 to rule out the existence of (v, k, λ) difference set. Examples of such parameters are listed in Tables 1 and 3. We also listed partial results in Tables 2, 4, and 5.

References

[1] D. Jungnickel, A. Pott, and K. W. Smith, "Difference sets," in *The CRC Handbook of Combinatorial Designs, Preprint*, C. J. Colbourn and J. H. Dinitz, Eds., CRC Press, 2005.

[2] K. T. Arasu, "On Lander's conjecture for the case $\lambda = 3$, J," in *Proceedings of the 1st Carbondale Combinatorics Conference*, vol. 1, pp. 5–11, 1987.

[3] K. T. Arasu and S. K. Sehgal, "Non-existence of some difference sets," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 32, pp. 207–211, 2000.

[4] L. D. Baumert, *Cyclic Difference Sets*, vol. 182 of *Lecture Notes in Mathematics*, Springer, Berlin, Germany, 1971.

[5] J. F. Dillon, "Variations on a scheme of McFarland for noncyclic difference sets," *Journal of Combinatorial Theory. Series A*, vol. 40, no. 1, pp. 9–21, 1985.

[6] M. Hall, Jr., *Combinatorial Theory*, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons, New York, NY, USA, 2nd edition, 1986, A Wiley-Interscience Publication.

[7] J. E. Iiams, "Lander's tables are complete," in *Difference Sets, Sequences and Their Correlation Properties*, vol. 542, pp. 239–257, Klumer Academic, Dordrecht, The Netherlands, 1999.

[8] Y. J. Ionin and M. S. Shrikhande, *Combinatorics of Symmetric Designs*, vol. 5 of *New Mathematical Monographs*, Cambridge University Press, Cambridge, UK, 2006.

[9] D. Jungnickel and A. Pott, "Difference sets: an introduction," in *Difference Sets, Sequences and Their Correlation Properties*, vol. 542, pp. 259–295, Klumer Academic, Dordrecht, The Netherlands, 1999.

[10] L. E. Kopilovich, "Difference sets in noncyclic abelian groups," *Cybernetics*, vol. 25, no. 2, pp. 153–157, 1989.

[11] E. S. Lander, *Symmetric Designs: An Algebraic Approach*, vol. 74 of *London Mathematical Society Lecture Note Series*, Cambridge University Press, Cambridge, UK, 1983.

[12] A. Pott, *Finite Geometry and Character Theory*, vol. 1601 of *Lecture Notes in Mathematics*, Springer, Berlin, Germany, 1995.

[13] B. Schmidt, "Cyclotomic integers and finite geometry," *Journal of the American Mathematical Society*, vol. 12, no. 4, pp. 929–952, 1999.

[14] R. J. Turyn, "Character sums and difference sets," *Pacific Journal of Mathematics*, vol. 15, pp. 319–346, 1965.

[15] M. Hall, Jr., "Cyclic projective planes," *Duke Mathematical Journal*, vol. 14, pp. 1079–1090, 1947.

[16] K. T. Arasu and S. K. Sehgal, "On abelian difference sets," in *Algebra: Some Recent Advances*, pp. 1–27, Birkhäuser, Basle, Switzerland, 1999.

[17] D. R. Hughes, "Biplanes and semi-biplanes," in *Proceedings of the Australian Conference on Combinatorial Mathematics*, vol. 686 of *Lecture Notes in Mathematics*, pp. 55–58, Springer, Berlin, Germany, 1978.

[18] R. E. Kibler, "A summary of noncyclic difference sets," *Journal of Combinatorial Theory. Series A*, vol. 25, no. 1, pp. 62–67, 1978.

[19] A. V. López and M. A. G. Sánchez, "On the existence of abelian difference sets with $100 < k \leq 150$," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 23, pp. 97–112, 1997.

[20] B. Franklin and S. Sam, "Non existence of some cyclic difference sets," 2007.

[21] A. S. Osifodunrin, "On the existence of non-abelian (210, 77, 28), (336, 135, 54) and (496, 55,6) difference sets," *Discrete Mathematics, Algorithms and Applications*, vol. 3, no. 1, pp. 121–137, 2011.

[22] R. A. Liebler, "The inversion formula," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 13, pp. 143–160, 1993.

[23] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, A K Peters, Natick, Mass, USA, Third edition, 2002.

[24] S. L. Ma, "Planar functions, relative difference sets, and character theory," *Journal of Algebra*, vol. 185, no. 2, pp. 342–356, 1996.

[25] S. Lang, *Algebraic Number Theory*, Addison-Wesley Publishing, Reading, Mass, USA, 1970.

[26] O. Gjoneski, A. S. Osifodunrin, and K. W. Smith, on existence of (176, 50, 14) and (704, 38,2) difference sets, to appear.

[27] W. Ledermann, *Introduction to Group Characters*, Cambridge University Press, Cambridge, UK, 1977.

[28] M. Hall, Jr., *The theory of Groups*, The Macmillan Company, New York, NY, USA, 1959.