On Lander's Conjecture

for the Case $\lambda = 3$

by

K. T. Arasu
Department of Mathematics and Statistics
Wright State University
Dayton, Ohio 45435

ABSTRACT Lander conjectured: If D is a (v,k,λ) difference set in an abelian group G with a cyclic Sylow p-subgroup, then p does not divide (v,n), where $n = k-\lambda$.

Various nonexistence theorems are used to verify the above conjecture (all hand calculations) for $k \leq 500$, except for $k = 228$, 282 and 444, when $\lambda = 3$. Using a machine, it is possible to do the checking for large k.

1. Introduction.

Let G be an abelian group of order v. A (v,k,λ) difference set in G is a subset D of G of size k such that each element $g \neq 1$ of G appears exactly λ times in the list

$$(xy^{-1}: x, y \in D, x \neq y).$$

An easy counting shows that

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

or

$$\lambda v = (k-\lambda)(k+\lambda-1) + \lambda^2 \tag{2}$$

We refer the reader to [2] and [5] for an excellent treatment on the theory of difference sets and their multipliers.

For $\lambda = 1$, the parameters take the form $(n^2+n+1, n+1, 1)$ and an easy construction produces a projective plane of order n. In this case we have $(v,n)=1$. In general, for a (v,k,λ) difference set, we define $n = k-\lambda$.

Ryser's conjecture [7] If D is a (v,k,λ) difference set in a cyclic group G, then $(v,n) = 1$.

Remark: The assumption "cyclic" cannot be dropped, for instance $(16,6,2)$ difference sets exist in all noncyclic groups (including

JCMCC 1(1987), pp. 5–11

nonabelian) of order 16. (See [4]).

An improvement of the above is due to Lander.

Lander's Conjecture [5] If there exists a (v,k,λ) difference set in an abelian group G whose Sylow p-subgroup is cyclic, then p does not divide (v,n).

Clearly Lander's conjecture implies Ryser's.

For $\lambda = 1$, both these conjectures are clearly true. In this paper we study Lander's conjecture for the case $\lambda = 3$ and verify it for $k \leq 500$ except for $k = 228$, 282 and 444. For $k \leq 75$ and for any λ, Lander [5] has verified these conjectures. We look for triples (v,k,λ) which satisfy equations (1) and (2) with $\lambda = 3$, $k \leq 500$ and $(v,n) \neq 1$. Equation (2) implies that when $\lambda = 3$, the only prime that divides (v,n) is 3, in which case actually $9|n$. We use various nonexistence theorems to verify Lander's conjecture for these parameter triples.

2. Nonexistence results.

Theorem 1 (Mann [6]) Suppose that there exists a (v,k,λ) difference set D in a group G. If for some divisor w of v, $w > 1$, and some prime p, there exists an integer j such that

$$p^j \equiv -1 \pmod{w},$$

then p does not divide the square-free part of n.

Remark Theorem 1 was proved by Mann [6] when the underlying group is abelian. Lander [5] gives a proof of this which includes nonabelian difference sets as well.

Table 1 shows the parameters $(v,k,3)$ with $76 \leq k \leq 500$ excluded by this test. We only supply the value of k (v would then be determined by equation (1)).

TABLE 1

(v,k,3)	$p^f \equiv -1 \pmod{w}$
(v, 102, 3)	$11 \equiv -1 \pmod{3}$
(v, 138, 3)	$5 \equiv -1 \pmod{3}$
(v, 156, 3)	$17 \equiv -1 \pmod{3}$
(v, 174, 3)	$19 \equiv -1 \pmod{5}$
(v, 192, 3)	$3^2 \equiv -1 \pmod{5}$
(v, 210, 3)	$23 \equiv -1 \pmod{3}$
(v, 246, 3)	$3^9 \equiv -1 \pmod{37}$
(v, 264, 3)	$29 \equiv -1 \pmod{3}$
(v, 300, 3)	$11 \equiv -1 \pmod{3}$
(v, 318, 3)	$5 \equiv -1 \pmod{3}$
(v, 354, 3)	$3^2 \equiv -1 \pmod{5}$
(v, 372, 3)	$41 \equiv -1 \pmod{3}$
(v, 390, 3)	$43^{468} \equiv -1 \pmod{1873}$
(v, 408, 3)	$5 \equiv -1 \pmod{3}$
(v, 426, 3)	$47 \equiv -1 \pmod{3}$
(v, 462, 3)	$17 \equiv -1 \pmod{3}$
(v, 480, 3)	$53 \equiv -1 \pmod{3}$
(v, 498, 3)	$5 \equiv -1 \pmod{3}$

An integer a is said to be <u>semiprimitive</u> modulo m if $a^f \equiv -1 \pmod{m}$ for some integer f. A prime p is said to be <u>self-conjugate</u> (mod w) if p is semiprimitive (mod w_p), where w_p is the largest divisor of w relatively prime to p.

<u>Theorem 2</u> (Turyn [8]) Suppose that there exists a (v,k,λ) difference set D in an abelian group G. If p is a prime such that

(1) p divides v and n, and

(2) p is self-conjugate (mod exponent of G), then the Sylow p-subgroup of G is not cyclic.

Application The (v, 120, 3) abelian differnce set, where $v = 3^2 23^2$, does not exist in the group G whose Sylow 3-subgroup is cyclic.

Proof: Apply theorem 2, noting that $3^{253} \equiv -1 \pmod{23^2}$.

Theorem 3 (Mann [6]) Let D be a (v,k,λ) difference set in an abelian group G. Suppose that -1 is a G/H - multiplier for some proper subgroup H. Then either n is a square or for some prime p,

(1) the square-free part of n is p

(2) the order of G/H is a power of p and

(3) $p \equiv 1 \pmod 4$.

Theorem 4 (Arasu) If there exists an abelian (v,k,3) difference set with $(v,n) \neq 1$ and n a nonsquare, then n must be odd. Furthermore, each prime divisor p of n, $p \neq 3$, satisfies the following:

(1) $\exp_v(p)$ is odd, and

(2) For each divisor h of v,

$$h\,(-1)^{\frac{h-1}{2}}$$

is a square in the ring of p-adic integers.

Proof: Let D be an abelian (v,k,3) difference set where $(v,n) \neq 1$ and n a nonsquare. We note that (v,n) = 3, in view of equation (2). If possible, suppose that n is even.

Case 1 $n \equiv 2 \pmod 4$. Then 2 divides the square-free part of n and $2 \equiv -1 \pmod 3$. This contradicts theorem 1, taking w = 3.

Case 2 $n \equiv 0 \pmod 4$. By Bruck's multiplier theorem [3], 2 is a multiplier of D. Let H be a subgroup of G of index 3. Then -1 is a G/H-multiplier of D, but the order of G/H is 3, which is not

congruent to 1 (mod 4), contradicting theorem 3.

This proves the first part of theorem 4. The second part of theorem (4) can be proved using the ideas of (1).

Applications (v,k,3) abelian difference sets do not exist whenever k is odd and (v,n) ≠1, n a nonsquare.

Proof: Follows from theorem 4, as n is even.

Theorem 5 (Lander [5]) Let D be a (v,k,λ) difference set in an abelian group G. Let p be a prime dividing n and v. Let K be a proper subgroup of G, containing the Sylow p-subgroup. Suppose that there exists a numerical G/K-multiplier t such that

$$tp^j \equiv -1 \pmod{\text{exponent of } G/K} \text{ for some integer } j.$$

Then for some integer i, we have $p^{2i} \| n$, $p^i \| k$, $p^i \| \lambda$ and $p^i | v$. Moreover, if K is the Sylow p-subgroup of G, then in fact $p^{i+1} | v$.

Application (v, 84, 3), where $v = 5^2 \cdot 3 \cdot 31$, abelian difference sets do not exist.

Proof Let K be a subgroup of G of index 31. Then K contains the Sylow 3-subgroup of G. Take p = 3 in theorem 5. Since $3^{15} \equiv -1 \pmod{31}$, result follows from theorem 5, choosing t = 1.

Theorem 6 (Lander [5]) Suppose that there exists a (v,k,λ)-difference set in an abelian group G. Let H be a subgroup of order h and index w. Suppose that for some positive integer m,

(1) m^2 divides n

(2) m divides k, λ and w

(3) m is self-conjugate (mod exponent of G/H),

and (4) if p is a prime dividing m and w, then the Sylow p-subgroup of G/H is cyclic.

Then,

$$h \geq \frac{1}{m} + \left(\frac{k}{\lambda}\right)\left(\frac{m-1}{m}\right).$$

Application (v, 336,3), where $v = 3^2 \cdot 11 \cdot 379$, abelian difference

sets do not exist in Z_v.

Proof: Take m = 3, h = 11, $w = 3^2 \cdot 379$, and p = 3 in theorem 6. Since $3^{189} \equiv -1 \pmod{379}$, theorem 6 applies and the result follows.

3. Conclusion

The results of section 2 supports Lander's conjecture for all $k \leq 500$, except k = 228, k = 282 and k = 444, when $\lambda = 3$. Possible counterexamples may exist to disprove Lander's (and hence Ryser's) conjecture for these three exceptional values, but we believe the contrary. Known nonexistence results do not suffice to settle these three cases.

Finally we wish to mention that all the results of this paper can be generalized to other values of λ in a straightforward manner.

Acknowledgement

The author would like to thank Mr. Ashok Vijayabhanu, Director of National Institute of Computer Education, Madras, India, for his valuable time spent in checking all the calculations that appear in this manuscript.

REFERENCES

1. Arasu, K. T., "On abelian difference sets", submitted.
2. Beth, Th., Jungnickel, D. and Lenz, H., Design Theory Bibliographisches Institut Mannheim - Wien-Zurich, B. I. Wissenschaftsverlag (1985).
3. Bruck, R. H., "Difference sets in a finite group", Trans Amer Math Soc 78 (1955), 464-481.

4. Kibler, R. E., "A Summary of non-cyclic difference sets, k < 20", J. Comb Theory (A), 25(1978), 62-67.

5. Lander, E. S., Symmetric Designs: An Algebraic Approach, London Math Society Lecture note series 74, Cambridge, Cambridge University Press (1983).

6. Mann, H. B., "Balanced incomplete block designs and abelian difference sets", Ill J. Math., 8(1964), 252-261.

7. Ryser, H., Combinatorial Mathematics, Carus Mathematical Monographs, No. 14, (1963).

8. Turyn, R. "Character sums and differnece sets", Pac. J. Math., 15(1965), 319-346.