BULL. AUSTRAL. MATH. SOC. 05B30
VOL. 10 (1974), 321-323.

Adders for the patterned starter in some non-abelian groups

Philip A. Leonard

Starters with adders in abelian groups of odd order have been used extensively in the construction and study of Room squares. It is possible to define these concepts in non-abelian groups, with similar applicability to Room squares. Examples are given of adders for the "patterned starter" in the non-abelian groups of order pq , p and q primes larger than 3 , $p \equiv q \equiv 3 \pmod 4$, $q \equiv 1 \pmod p$.

One fruitful approach to the construction and study of Room squares has been that based on starters and adders in groups of odd order (see [2]).

If G is a multiplicative group of order $2n + 1$, and $H = G\backslash\{1\}$, a *starter* in G is a set $X = \{(x_i, y_i) \mid 1 \le i \le n\}$ of ordered pairs such that

$$H = \{x_i, y_i \mid 1 \le i \le n\} = \left\{x_iy_i^{-1}, y_ix_i^{-1} \mid 1 \le i \le n\right\} .$$

If X is a starter in G , an *adder* for X is an ordered set $A = (a_1, \ldots, a_n)$ of distinct elements of H such that

$$H = \{x_ia_i, y_ia_i \mid 1 \le i \le n\} .$$

Given a starter X with adder A_X , a Room square of side $2n + 1$ may be constructed as follows: let R be a square array, with rows and

Received 4 December 1973.

https://doi.org/10.1017/S0004972700041009 Published online by Cambridge University Press

and columns indexed by the elements of G. The cell in position (g, h) is empty unless $h = a_i g$ for some i, and in this case it contains the pair $\{x_i a_i g, y_i a_i g\}$.

This note contains examples of starters with adders in certain non-abelian groups (see [2], Problem 9).

Let p and q be odd primes, larger than 3, with $p \equiv q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod p$, and let G be the non-abelian group of order pq defined by $a^p = 1$, $b^q = 1$, $a^{-1}ba = b^r$, where r is an integer of order p (modulo q) (see [1]). Products in G are given by

$$a^x b^y \cdot a^u b^v = a^{x+u} b^{yr^u+v}, \quad 0 \le x, u \le p-1, \ 0 \le y, v \le q-1 .$$

Let R_p (respectively N_p) denote the set of quadratic residues (respectively non-residues) modulo p, with R_q and N_q defined similarly. Let

$$S = \left\{g = a^x b^y \mid x \in R_p \text{ , or, } x = 0 \text{ and } y \in R_q\right\} .$$

Since $p \equiv q \equiv 3 \pmod 4$, we have the following

LEMMA. *$X = \{(g, g^{-1}) \mid g \in S\}$ is a starter in G.*

The starter X of the lemma is called the *patterned starter* in G. Examples of adders for X are given in the following result. The proof, which is a routine matter of verification, is omitted.

THEOREM. *For $m \in N_p \backslash \{-1\}$ and $n \in N_q \backslash \{-1\}$, define k by $k \equiv \frac{m+1}{m-1} \pmod p$, and l by $l \equiv \frac{n+1}{n-1} \pmod q$. Then $A_X = (h_g)$, $g \in S$, with $h_g = a^{kx} b^{ly}$ for $g = a^x b^y$, is an adder for the patterned starter X, provided $l^p \not\equiv \pm 1 \pmod q$.*

For example, with $p = 7$ and $q = 67$, we may take $m = n = 3$, giving $k = l = 2$, which is suitable as $2^7 \equiv 61 \pmod{67}$. For the smallest eligible values of p and q, namely $p = 7$ and $q = 43$, $l = 2$ is not admissible, but $l = 3$ (corresponding to $n = 2$) is, as

https://doi.org/10.1017/S0004972700041009 Published online by Cambridge University Press

$3^7 \equiv 36 \pmod{43}$.

References

[1] Marshall Hall, Jr, *The theory of groups* (The Macmillan Company, New York, 1959).

[2] W.D. Wallis, "Room squares", *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, 33-121 (Lecture Notes in Mathematics, **292**. Springer-Verlag, Berlin, Heidelberg, New York, 1972).

Department of Mathematics,
Arizona State University,
Tempe,
Arizona,
USA.

https://doi.org/10.1017/S0004972700041009 Published online by Cambridge University Press