A Family of $N \times N$ Tuscan-2 Squares with $N+1$ Composite

B. A. Anderson
Department of Mathematics
Arizona State University
Tempe, Arizona 85287

Abstract. Golomb and Taylor (joined later by Etzion) have modified the notion of a complete Latin square to that of a Tuscan-k square. A Tuscan-k square is a row Latin square with the further property that for any two symbols a and b of the square, and for each m from 1 to k, there is at most one row in which b is the m^{th} symbol to the right of a. One question unresolved by a series of papers of the authors mentioned was whether or not $n \times n$ Tuscan-2 squares exist for infinitely many composite values of $n+1$. It is shown here that if p is a prime and $p \equiv 7 \pmod{12}$ or $p \equiv 5 \pmod{24}$, then Tuscan-2 squares of side $2p$ exist. If $p \equiv 7 \pmod{12}$, clearly $2p+1$ is always composite and if $p \equiv 5 \pmod{24}$, $2p+1$ is composite infinitely often. The squares constructed are in fact Latin squares that have the Tuscan-2 property in both dimensions.

Introduction.

The series of papers [9], [10], [11] has raised a number of interesting questions related to the idea of a complete Latin square. A Latin square $L = (l_{ij})$ of order n is *row complete* [*column complete*] iff the $n(n-1)$ ordered pairs $(l_{ij}, l_{i,j+1})$ $[l_{ij}, l_{i+1,j}]$ are all distinct. A Latin square is *complete* iff it is both row and column complete. These squares are useful in designing certain experiments where it is necessary to consider the interaction of nearest neighbors [8], [11].

According to [10], an *Italian square* is an $n \times n$ array in which each of the symbols $1, 2, \cdots, n$ appears exactly once in each row. A *Tuscan-k* square is an Italian square such that for any two symbols a and b and for each m, $1 \leq m \leq k$, there is at most one row in which b is the m^{th} symbol to the right of a. Thus a Tuscan-1 square is a row complete (not necessarily Latin) Italian square. Tuscan-1 squares are known to exist [15] for all n, $n \neq 3, 5$. It has been verified [11] that $n \times n$ Tuscan-$(n-1)$ arrays exist whenever $n+1 = p$ is prime (use the multiplication table of non-zero elements of the finite field with p elements) and [10] that Tuscan-2 squares exist for all even n, $4 \leq n = 2m \leq 50$. For all these cases except $n = 8$, the "symmetric polygonal path" method [10] can be used. Symmetric polygonal paths are special cases of the following idea.

Suppose G is a finite group of order n with identity e. A *sequencing* [12] of G is an ordering $e, a_2, \ldots, a_n$ of all elements of G such that the partial products $e, ea_2 = b_2, ea_2a_3 = b_3, \ldots ea_2 \cdots a_n = b_n$ are distinct and hence also all of G. Attention will be restricted to a particular type of sequencing.

Definition 1: Suppose G is a group of order $2n$ with identity e and unique element z of order 2. A sequencing α

$$\alpha : e, a_2, \ldots, a_n, a_{n+1}, \ldots, a_{2n}$$
$$\beta : e, b_2, \ldots, b_n, b_{n+1}, \ldots, b_{2n}$$

with associated partial product sequence β will be called a *symmetric sequencing* [1] iff $a_{n+1} = z$ and for $1 \le i \le n-1$, $a_{n+1+i} = (a_{n+1-i})^{-1}$.

It is easy to see that the symmetric polygonal paths of [10] are the partial sum sequences associated with symmetric sequencings of Z_{2n}, the cyclic group of order $2n$.

Polygonal paths and rotation are used in [10] to construct Tuscan-1 squares. Stated in terms of sequencings [10, Lemma C1] says that every sequencing of Z_{2n} generates a Tuscan-1 square. In fact, one can do better than this by rearranging rows.

Theorem 1 [12]. *If G is a sequenceable group of order n with sequencing α and associated partial product sequence β, then the $n \times n$ array whose $(i,j)^{th}$ cell contains $b_i^{-1} b_j$ is a complete Latin square.*

This means that sequencings give arrays that have the Tuscan-1 property in both dimensions. For information on sequencings, see [3], [4], [5], [13].

One conjecture in [10] is that for all even n, $n \ge 4$, an $n \times n$ Tuscan-2 square exists. However, this has not been verified; in fact, it has not previously been established for so much as an infinite class of values n such that $n+1$ is composite. The goal of this paper is to exhibit such a class.

If G is a finite group with unique element z of order 2, define

$$F_{inv} = \{\{x, x^{-1}\} : x \in G \setminus \{e, z\}\}.$$

Definition 2: Suppose α is a symmetric sequencing of a group G of order $2n$ and for each i, $3 \le i \le n+1$, $A_i = a_{i-1} \cdot a_i$. The statement that α is a *symmetric T_2-sequencing* of G means that $\{A_3, A_4, \ldots, A_{n+1}\}$ is a transversal of F_{inv}.

Definition 3: A Latin Square L is *2-complete* iff it is Tuscan-2 in both dimensions (horizontally left-to-right and vertically top-to-bottom).

It will be useful to examine the construction of Theorem 1 in detail.

Remark 2. *Suppose G, α and β are as in Theorem 1 and $C = (c_{ij}) = (b_i^{-1} b_j)$ is the associated complete Latin square.*

i) $c_{ij} = c_{ji}^{-1}$ *(C is skew)*
ii) *Row 1 of C contains the elements of β in order.*
iii) *Row i of C is the left translate of Row 1 by b_i^{-1}.*
iv) *Column 1 of C is (Row 1)$^{-1}$*
v) *Column j of C is the right translate of column 1 by b_j.*

Proof: The arguments are straightforward.

Note that if b_j and b_{j+1} are consecutive elements in row 1, then $b_j(b_j^{-1} b_{j+1}) = b_{j+1}$. Similarly, if $b_i^{-1} b_j$ and $b_i^{-1} b_{j+1}$ are consecutive elements of row i, then as before, $b_i^{-1} b_j (b_j^{-1} b_{j+1}) = b_i^{-1} b_{j+1}$. Since $b_j^{-1} b_{j+1} = a_{j+1}$, an easy translation argument can be used to show horizontal completeness. On the other hand, suppose b_i^{-1} and b_{i+1}^{-1} are consecutive elements in column 1. Then $b_i^{-1}(b_i b_{i+1}^{-1}) = b_{i+1}^{-1}$ while if $b_i^{-1}b_j$ and $b_{i+1}^{-1}b_j$ are consecutive elements in column j, then

$$b_i^{-1}b_j[b_j^{-1}(b_i b_{i+1}^{-1})b_j] = b_{i+1}^{-1}b_j$$

and a translation argument is not so clear. Nevertheless, an easy argument for completeness exists [12]. It will be exhibited in 2-completeness form below.

Theorem 3. *If G is a finite group of order n with symmetric T_2-sequencing α and associated partial product sequence β, then the array $C = (c_{ij}) = (b_i^{-1}b_j)$ is a 2-complete $n \times n$ Latin square.*

Proof: By Theorem 1, C is a complete Latin square. Extend the limits of i in Definition 2 to $3 \leq i \leq 2n$ and it is easy to see that for $1 \leq i \leq n-1$,

$$A_{n+1+i} = A_{n+2-i}^{-1}$$

so that $\{A_3, \ldots, A_{n+1}, \ldots, A_{2n}\} = G \setminus \{e, z\}$.

The following argument shows vertical 2-completeness. Horizontal 2-completeness is verified similarly.

Suppose $c_{st} = c_{uv}$, and $c_{s+2,t} = c_{u+2,v}$. Then

$$b_s^{-1}b_t = b_u^{-1}b_v$$

and

$$b_{s+2}^{-1}b_t = b_{u+2}^{-1}b_v \text{ so that } b_t^{-1}b_{s+2} = b_v^{-1}b_{u+2}.$$

It follows that $b_s^{-1}b_{s+2} = b_u^{-1}b_{u+2}$. Since $b_s^{-1}b_{s+2} = A_{s+2}$ and $b_u^{-1}b_{u+2} = A_{u+2}$, $s = u$ by properties of the sequencing. Then $b_s^{-1}b_t = b_s^{-1}b_v$ so that $b_t = b_v$ and $t = v$.

Example 1. A symmetric T_2-sequencing α of Z_6. The T_2-row contains A_3, A_4, A_5 and A_6.

T_2			5,	4,	2,	1
α:	0,	4,	1,	3,	5,	2
β:	0,	4,	5,	2,	1,	3

Figure 1 shows the Tuscan-2 Latin square that arises from α via the rotation construction of [10]. Note that this square is not 2-complete or complete. Figure 2 gives the 2-complete Latin square that arises from α via Gordon's construction.

0	4	5	2	1	3
1	5	0	3	2	4
2	0	1	4	3	5
3	1	2	5	4	0
4	2	3	0	5	1
5	3	4	1	0	2

Figure 1

0	4	5	2	1	3
2	0	1	4	3	5
1	5	0	3	2	4
4	2	3	0	5	1
5	3	4	1	0	2
3	1	2	5	4	0

Figure 2

In view of Theorem 3, the goal of this paper can be restated as the exhibition of a class of symmetric T_2-sequencings. This will be accomplished as follows. Only cyclic groups Z_{2p}, p an odd prime, will be considered. In this type of situation, it is often useful to be able to compute in a field. Thus, the plan will be to factor down to Z_p and Z_2 and look for images of symmetric T_2-sequencings on Z_{2p}. When a symmetric sequencing on Z_{2p} is "projected" to Z_p [3], the result is a 2-sequencing (to be defined later). Projecting the other way to Z_2 corresponds to asking how to lift the 2-sequencing back to a symmetric sequencing of Z_{2p}.

A certain class of possible 2-sequencings that arise when p is an odd prime will be analyzed. Many elements in this class are 2-sequencings and some have an additional property (to be defined later) necessary if they are to be images of symmetric T_2-sequencings. Most of the elements having this additional property cannot be lifted to symmetric T_2-sequencings of Z_{2p} but, after all the sifting is completed, a few gold nuggets remain.

The Construction.

The first order of business is to characterize certain symmetric T_2-sequencings in terms of the factorization process described above.

Definition 4: Suppose H is a finite group of order n with identity e. A *2-sequencing* [3], [7] γ of H is an ordering $e, c_2, \ldots, c_n$ of certain elements of H (not necessarily distinct) such that

i) the associated partial products

$$\delta : e, ec_2, ec_2c_3, \ldots, ec_2c_3 \cdots c_n$$

are distinct and hence all of H,

ii) if $y \in H$ and $y \neq y^{-1}$, then

$$|\{i : 2 \leq i \leq n \text{ and } (c_i = y \text{ or } c_i = y^{-1})\}| = 2,$$

(this will be referred to as the "two occurrence property")

iii) if $y \in H$ and $y = y^{-1}$, then

$$|\{i : 1 \leq i \leq n \text{ and } c_i = y\}| = 1.$$

Definition 5: Suppose H is a finite group of odd order n and $\gamma : e, c_2, c_3, \ldots, c_n$ is a 2-sequencing of H. For each i, $3 \leq i \leq n$, let $C_i = c_{i-1} \cdot c_i$ and define $C_{n+1} = c_n$. The statement that γ is a t_2 *2-sequencing* of H means that if $y \in H \setminus \{e\}$, then

$$|\{i : 3 \leq i \leq n+1 \text{ and } (C_i = y \text{ or } C_i = y^{-1})\}| = 2.$$

The symbol t_2 will denote the row $C_3, C_4, \ldots, C_n, C_{n+1}$ so that row t_2 of a t_2 2-sequencing has the two occurrence property.

If γ is a 2-sequencing of H and c_i and c_j satisfy Definition 4 (ii) with respect to y, the phrase "c_i and c_j are the two occurrences of $\{y, y^{-1}\}$ in γ" will be used.

Definition 6: Suppose γ is a t_2 2-sequencing of the odd order group H. Let

$$\sigma : 0, \sigma_2, \sigma_3, \ldots, \sigma_n, 1$$

be a sequence of length $n+1$ of elements of Z_2 with associated partial sum sequence

$$\rho : 0, \rho_2, \rho_3, \ldots, \rho_n, \rho_{n+1}.$$

For $3 \leq i \leq n+1$, let $\sum_i = \sigma_{i-1} + \sigma_i \pmod 2$ and let τ_2 be the sequence $\sum_3, \sum_4, \ldots, \sum_{n+1}$. The statement that σ is *compatible* with γ means that

i) $\sigma_1 = 0$ and $\sigma_{n+1} = 1$,
ii) if $y \in H \setminus \{e\}$ and c_i and c_j are the two occurrences of $\{y, y^{-1}\}$ in γ, then $\sigma_i \neq \sigma_j$,
iii) if $y \in H \setminus \{e\}$ and C_u and C_v are the two occurrences of $\{y, y^{-1}\}$ in t_2, then $\sum_u \neq \sum_v$.

Remark 4. *If σ is compatible with γ, then*

i) *σ contains $(n+1)/2$ 0's and $(n+1)/2$ 1's,*
ii) *τ_2 contains $(n-1)/2$ 0's and $(n-1)2$ 1's.*

Before proceeding to the characterization theorem, an example will serve to illustrate the definitions. The following symmetric T_2-sequencing of Z_{10} is taken from [10] although exhaustive lists of symmetric sequencings of low order cyclic groups have been known for some time [2].

	T_2	3, 6, 1, 2, 8, 9, 4,7
Z_{10}:	α:	0, 1, 2, 4, 7, 5, 3, 6, 8, 9
	β:	0, 1, 3, 7, 4, 9, 2, 8, 6,5

Let $H = Z_5$ and project down to a t_2 2-sequencing of Z_{10}/Z_2 and a compatible sequence σ of six elements of Z_2.

	t_2:	3 1 1 2			τ_2;	1 0 1 0
Z_5:	γ:	0, 1, 2, 4, 2		Z_2:	σ:	0, 1, 0, 0, 1, 1
	δ:	0, 1, 3, 2, 4			ρ:	0, 1, 1, 1, 0, 1

Lemma 5. *Suppose G is a group of order $2n$, n odd, with a unique element z of order 2. Then*

i) *G has a subgroup H of order n,*
ii) *$z \notin H$,*
iii) *$x \in H$ iff $xz \notin H$ (which occurs iff $x^{-1}z \notin H$).*

Proof: Only (i) requires an argument. Since n is odd, the Sylow-2 subgroup of G is Z_2 and the result follows by [14, Corollary 1, p. 144].

Theorem 6. *Suppose G is a group of order $2n$, n odd, with a unique element z of order 2. Then G has a symmetric T_2-sequencing iff*

i) *G/Z_2 has a t_2 2-sequencing γ and*
ii) *γ has a compatible 0-1 sequence σ.*

Proof: First let α be a symmetric T_2-sequencing of G and let π be the natural projection from G to G/Z_2. By [3], $(\pi(e), \pi(a_2), \ldots, \pi(a_n)) = \pi[\alpha]$ is a 2-sequencing of G/Z_2. Consider a coset $y = \{x, xz\} \in G/Z_2$, $x \notin \{e, z\}$. The inverse coset is $y^{-1} = \{x^{-1}, x^{-1}z\}$ and these two cosets are distinct since n is odd. Now

$$y \cup y^{-1} = \{x, xz\} \cup \{x^{-1}, x^{-1}z\} = \{x, x^{-1}\} \cup \{xz, x^{-1}z\} \subset F_{inv}.$$

By hypothesis, $\{A_3, \ldots, A_{n+1}\}$ contains exactly one element from $\{x, x^{-1}\}$ and exactly one element from $\{xz, x^{-1}z\}$. Thus $\{y, y^{-1}\}$ occurs exactly twice in

$$\{\pi(A_3), \ldots, \pi(A_{n+1})\} = \{C_3, \ldots, C_{n+1}\}.$$

Since this holds for any pair $\{y, y^{-1}\} \in (G/Z_2 \setminus \{e, z\})$, $\pi[\alpha] = \gamma$ is a t_2 2-sequencing of G/Z_2.

Now construct the compatible 0-1 sequence σ. Let H be a subgroup of G of order n and let π_2 be the natural projection from G to $G/H \approx Z_2$ where H is denoted by 0 and Hz by 1. Then $\pi_2(e), \pi_2(a_2), \ldots, \pi_2(a_{n+1})$ is a sequence of 0's and 1's and clearly $\pi_2(e) = \sigma_1 = 0$ and, since $a_{n+1} = z$, $\sigma_{n+1} = 1$.

Suppose c_i and c_j are the two occurrences of $\{y, y^{-1}\}$ in γ. Since $\pi(a_i) = c_i$ and $\pi(a_j) = c_j$, $\sigma_i \neq \sigma_j$ if it can be shown that $\{a_i, a_j\}$ is a transversal of $\{H, Hz\}$. There are two possibilities. If $\pi(a_i) = \pi(a_j) = \{x, xz\}$, then since α is a symmetric sequencing, $a_i \neq a_j$ and the result follows from Lemma 5 (iii). If, on the other hand, $\pi(a_i) = \{x, xz\}$ and $\pi(a_j) = \{x^{-1}, x^{-1}z\}$, then it is easy to see [3] that since α is a symmetric sequencing,

$$a_i = x \text{ implies } a_j = x^{-1}z$$
$$a_i = xz \text{ implies } a_j = x^{-1}$$

and the result again follows from Lemma 5 (iii).

To complete the first half of the argument, suppose C_u and C_v are the two occurrences of $\{y, y^{-1}\}$ in t_2. Since $\pi(A_u) = C_u$ and $\pi(A_v) = C_v$, $\sum_u \neq \sum_v$ if it can be shown that $\{A_u, A_v\}$ is a transversal of $\{H, Hz\}$. Again there are two possibilities. If $\pi(A_u) = \pi(A_v) = \{x, xz\}$ then since $\{A_3, \ldots, A_{n+1}\}$ is a transversal of F_{inv}, $A_u \neq A_v$ and the result follows as before. If, on the other hand, $\pi(A_u) = \{x, xz\}$ and $\pi(A_v) = \{x^{-1}, x^{-1}z\}$, then

$$A_u = x \text{ implies } A_v = x^{-1}z$$
$$\text{and } A_u = xz \text{ implies } A_v = x^{-1}$$

so that the first half of the proof is complete.

Suppose, conversely, that γ is a t_2 2-sequencing of G/Z_2 and there is a compatible 0-1 sequence σ on $G/H \approx Z_2$. By [3], γ can be lifted to a class of symmetric sequencings of G. It is easy to see that the compatibility of γ and σ implies there is a unique lift that projects to both γ and σ. Call this symmetric sequencing α. The argument will be complete if it can be shown that $\{A_3, \ldots, A_{n+1}\}$ is a transversal of F_{inv}. If this is not the case, then by the pigeonhole principle, either

i) there exist $i \neq j$ such that $A_i = A_j$ or
ii) there exist $i \neq j$ such that $A_i^{-1} = A_j$.

Similar methods handle both these cases so consider (ii). In this situation $\pi(A_i) = \{A_i, A_i z\} = y$ and $\pi(A_j) = \{A_i^{-1}, A_i^{-1}z\} = y^{-1}$ are the two occurrences of $\{y, y^{-1}\}$ in t_2. By compatibility $\sum_i \neq \sum_j$ and this implies A_i and A_j are in different cosets of H, a contradiction. This completes the argument for Theorem 6.

It will be useful to establish some notation as an aid to describing the class of 2-sequencings to be considered. If p is an odd prime,

$$PS = \{\{x, -x\} : x \in Z_p \setminus \{0\}\}$$

$S_1 : 1, 2, 3, \ldots, (p-1)/2$ $\qquad$ $\widehat{S}_1 : 0, 1, 2, 3, \ldots, (p-1)/2$

$S_2 : (p-1)/2, \ldots, 3, 2, 1$ $\qquad$ $xS_2 : [(p-1)/2]x, \ldots, 3x, 2x, x; x \in Z_p \setminus \{0\}$

$s : \widehat{S}_1, xS_2$

Clearly s is a "sequence" (it is the concatenation of two *ordered* sets) of p elements of Z_p. It will be of interest to determine when s is a 2-sequencing of Z_p.

Remark 7. *If $x \in Z_p \setminus \{0\}$, then S_1 and xS_2 are transversals of PS.*

Consider s in detail along with its associated partial sum sequence t.

$$s : 0, 1, 2, 3, \ldots, (p-1)/2, [(p-1)/2]x, [(p-3)/2]x, \ldots, 3x, 2x, x$$
$$t : 0, 1, 3, 6, \ldots, (p^2-1)/8, \ldots$$

Let Γ_1 denote the first $(p-1)/2$ elements of t and let Γ_2 denote the last $(p-1)/2$ elements of t. Note that the occurrence of $(p^2-1)/8$ in the middle position of t is missed in the definition of Γ_1 and Γ_2 and that $\Gamma_1, \Gamma_2 \subset Z_p$. Let Q denote the quadratic residues mod p and let N denote the quadratic non-residues mod p. As usual, if $A, B \subset Z_p$ and $x \in Z_p$, $A+x = \{a+x : a \in A\}$ and $xA = \{xa : a \in A\}$.

Lemma 8. *With $s : \widehat{S}_1, xS_2$ defined as above, the following results hold.*

i) $\Gamma_1 = Q + (p^2-1)/8$ *if* $p \equiv \pm 1 \pmod 8$,
$\Gamma_2 = -xQ + (p^2-1)/8$ *if* $p \equiv \pm 1 \pmod 8$.
ii) $\Gamma_1 = N + (p^2-1)/8$ *if* $p \equiv \pm 3 \pmod 8$,
$\Gamma_2 = -xN + (p^2-1)/8$ *if* $p \equiv \pm 3 \pmod 8$.

Proof: Consider Γ_1 first. The elements g_{n+1} of Γ_1 have the form $g_{n+1} = n(n+1)/2, 0 \leq n \leq (p-3)/2$. But

$$\frac{n(n+1)}{2} = \frac{(n+1/2)^2 - 1/4}{2} = \frac{4(n+1/2)^2 - 1}{8} = \frac{4[(n+1) - 1/2]^2 - 1}{8}$$

and $2^{-1} = (p+1)/2$. Since $1 \leq n+1 \leq (p-1)/2$

$$\begin{aligned}(n+1) - 1/2 &\in \{1,2,\ldots,(p-1)/2\} - (p+1)/2 \\ &= \{-1,-2,\ldots,-(p-1)/2\}.\end{aligned}$$

Thus

$$\Gamma_1 = (4Q-1)/8 = (Q-1)/8 = Q\cdot 8^{-1} - 8^{-1} = Q\cdot 8^{-1} + (p^2-1)/8.$$

Now $2 \in Q$ if $p \equiv \pm 1 \pmod 8$ and $2 \in N$ if $p \equiv \pm 3 \pmod 8$ [6] so the results relative to Γ_1 are clear.

In order to compute Γ_2 look at the elements in the s-row above the members of Γ_2. The sum of the first i elements here can be thought of as the sum of all these elements minus the sum of the elements following the first i elements. For example, with $i = 1$

$$[(p-1)/2]x = [(p^2-1)/8 - (p-1)(p-3)/8]x.$$

It follows that (with $(p^2-1)/8 = \omega$)

$$\Gamma_2 = \{\omega + x[\omega - (p-1)(p-3)/8], \ldots, \omega + x[\omega - 1\cdot 2/2], \omega + x[\omega - 0]\}. \quad (1)$$

Without the translation by ω, (1) becomes

$$\{x[\omega - (p-1)(p-3)/8], \ldots, x[\omega - 1\cdot 2/2], x[\omega - 0]\}. \quad (2)$$

Without the multiplication by x, (2) becomes

$$\{[\omega - (p-1)(p-3)/8], \ldots, [\omega - 1\cdot 2/2], [\omega - 0]\}. \quad (3)$$

Without the translation by ω, (3) becomes (in reverse order)

$$\{-0, -1, -3, \ldots, -(p-3)(p-1)/8\}. \quad (4)$$

By the first part of the argument

$$(4) = \begin{cases} -Q - (p^2-1)/8 & \text{if } p \equiv \pm 1 \pmod 8 \\ -N - (p^2-1)/8 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

and the result follows by retracing the steps back up to (1).

Theorem 9. *With $s : \widehat{S}_1, xS_2$ defined as above, s is a 2-sequencing of Z_p iff*

i) $p \equiv 1 \pmod 4$ *and* $x \in N$ *or*
ii) $p \equiv 3 \pmod 4$ *and* $x \in Q$.

Proof: Recall that $-1 \in Q$ if $p \equiv 1 \pmod 4$ and $-1 \in N$ if $p \equiv 3 \pmod 4$ [6]. Lemma 8 gives four cases to be resolved. Since the arguments for all the cases are similar only one case will be presented here.

If $p \equiv 1 \pmod 8$, then

$$\Gamma_1 = Q + (p^2 - 1)/8 \text{ and } \Gamma_2 = -xQ + (p^2 - 1)/8.$$

Since

$$Z_p = Z_p + (p^2 - 1)/8 = [(Q \cup N)(p^2 - 1)/8] \cup [\{0\} + (p^2 - 1)/8]$$

s will be a 2-sequencing iff $-xQ = N$. Since $-1 \in Q$, this holds iff $x \in N$.

Lemma 10. *With $s : \widehat{S}_1, xS_2$ defined as above, the t_2 row associated with s has the two occurrence property of Definition 5 (independent of whether or not s is a 2-sequencing) iff $x \equiv 1, -3 \pmod p$.*

Proof: Clearly

$$\begin{aligned}\{C_3, C_4, \ldots, C_{(p+1)/2}\} &= \{3, 5, \ldots, p-2\}\\ \{C_{(p+5)/2}, \ldots, C_p\} \cup \{C_{p+1}\} &= \{(p-2)x, \ldots, 3x\} \cup \{x\}\\ C_{(p+3)/2} &= (1+x)(p-1)/2.\end{aligned}$$

Since $x\{1, 3, 5, \ldots, p-2\}$ is a transversal of PS, the t_2 row has the two occurrence property iff $(1+x)(p-1)/2 \equiv \pm 1 \pmod p$. Easy computations now give the result.

Theorem 11. *With $s : \widehat{S}_1, xS_2$ defined as above, $s = \gamma$ is a t_2 2-sequencing of Z_p iff*

i) $x \equiv 1 \pmod p$ *and* $p \equiv 3 \pmod 4$ *or*
ii) $x \equiv -3 \pmod p$ *and* $p \equiv 5, 7 \pmod{12}$.

Proof: Combine the results of Theorem 9 and Lemma 10. Use the facts that

$$\begin{aligned}&-1 \in Q \text{ if } p \equiv 1 \pmod 4, \qquad 3 \in Q \text{ if } p \equiv \pm 1 \pmod{12}\\ &-1 \in N \text{ if } p \equiv 3 \pmod 4, \qquad 3 \in N \text{ if } p \equiv \pm 5 \pmod{12}\end{aligned}$$

To begin, suppose s is a t_2 2-sequencing of Z_p. If $x \equiv 1 \pmod p$, then $x \in Q$ and by Theorem 9, $p \equiv 3 \pmod 4$. If $x \equiv -3 \pmod p$, then split things into two cases. Suppose first that $p \equiv 1 \pmod 4$. Then $-3 \in N$ by Theorem 9. If $-1 \in N$, then $p \equiv 3 \pmod 4$, a contradiction. Thus $-1 \in Q$, $3 \in N$ and $p \equiv \pm 5 \pmod{12}$. Since $p \equiv 7 \pmod{12}$ and $p \equiv 1 \pmod 4$ is not possible, $p \equiv 5 \pmod{12}$.

Lastly, suppose $p \equiv 3 \pmod 4$. Then $-3 \in Q$ by Theorem 9. If $-1 \in Q$, then $p \equiv 1 \pmod 4$, a contradiction. Thus $-1 \in N$, $3 \in N$ and $p \equiv \pm 5 \pmod{12}$. Since $p \equiv 5 \pmod{12}$ and $p \equiv 3 \pmod 4$ is not possible, $p \equiv 7 \pmod{12}$.

The converses are straightforward.

Interest now centers on the question of when the t_2 2-sequencings γ on Z_p promised by Theorem 11 can be lifted to symmetric T_2-sequencings of Z_{2p}. By Theorem 6 it will suffice to find compatible 0-1 sequences σ of length $p+1$. As will become clear shortly, compatibility induces considerable structure to the possible lifts in the case of the t_2 2-sequencings of Theorem 11.

Suppose H is a group of odd order n and γ is a t_2 2-sequencing of H.

Position:	1	2	3	...	n	$n+1$
t_2:			C_3	...	C_n	C_{n+1}
γ:	e,	c_2,	c_3,	...,	c_n	
δ:	e,	d_2,	d_3,	...,	d_n,	

By definition, both the t_2-row and the γ-row have the two occurrence property.

Definition 7: If γ is as above

$$F_\gamma = \{\{i,j\} : \exists y \in H \setminus \{e\} \ni c_i, c_j \text{ are the two occurrences of } \{y, y^{-1}\} \text{ in } \gamma\},$$
$$F_{t_2} = \{\{u,v\} : \exists y \in H \setminus \{e\} \ni C_u, C_v \text{ are the two occurrences of } \{y, y^{-1}\} \text{ in } t_2\}.$$

It is clear that F_γ is a partition of $\{2, 3, \ldots, n\}$ into pairs and F_{t_2} is a partition of $\{3, 4, \ldots, n+1\}$ into pairs.

What can be said about a compatible sequence σ?

Position:	1	2						$n-1$	n	$n+1$
T_2:					$\sum_k$	$\sum_u$	$\sum_v$			
σ:	0		σ_i	σ_{k-1}	σ_k	σ_j				1
ρ:										

By definition $\sigma_1 = 0$ and $\sigma_{n+1} = 1$. There are two very useful rules that can be described. Recall that $\sum_k = \sigma_{k-1} + \sigma_k$ in Z_2. Since this equation holds in a group, the following rule is valid.

2/3 Rule: If any two of the values in the equation $\sum_k = \sigma_{k-1} + \sigma_k$ are known, the third value is forced.

Compatibility gives another rule with two instances.

Disagreement Rule:

(1) If $\{i,j\} \in F_\gamma$ and σ_i is known, then σ_j is forced.
(2) If $\{u,v\} \in F_{t_2}$ and $\sum_u$ is known, then $\sum_v$ is forced.

It is now easy to settle the lifting question for one family of t_2 2-sequencings exhibited in Theorem 11.

Theorem 12. *Let γ_p be the t_2 2-sequencing of Z_p described in Theorem 11 when $p \equiv 3 \pmod 4$ and $x \equiv 1 \pmod p$. Then γ_p has a compatible 0-1 sequence σ_p iff $p = 3$.*

Proof: It is straightforward to compute that

$$F_{t_2} = \begin{cases} \{p+1,(p+3)/2\}, & \text{if } p=3 \\ \{p+1,(p+3)/2\},\{3,p\},\{4,p-1\},\ldots,\{(p+1)/2,(p+5)/2\}, & \text{if } p>3. \end{cases}$$

$$F_\gamma = \begin{cases} \{2,p\} = \{(p+1)/2,(p+3)/2\}, & \text{if } p=3 \\ \{2,p\},\{3,p-1\},\ldots,\{(p+1)/2,(p+3)/2\}, & \text{if } p>3. \end{cases}$$

What can be said about a compatible 0-1 sequence σ? The following diagram may be helpful.

Position:	1	2	3	4	...	$(p+3)/2$	...	$p-1$	p	$p+1$
τ_2:						1				0
σ:	0	0							1	1

Since $\{(p+1)/2,(p+3)/2\}$ is a consecutive pair in F_γ, the Disagreement Rule says $\sum_{(p+3)/2} = 1$ and this forces $\sum_{p+1} = 0$ which in turn yields $\sigma_p = 1$ by the 2/3 Rule and $\sigma_2 = 0$ by Disagreement. If $p = 3$, all entries are computed and the symmetric T_2-sequencing of Z_6 that results is the unique "symmetric polygonal path" example found in [10]. If $p > 3$, then the two possibilities for (σ_3, σ_{p-1}) [i.e., $(0,1)$ and $(1,0)$ by Disagreement] both lead to the conclusion $\sum_3 = \sum_p$ by the 2/3 Rule. This contradiction shows that there is no compatible 0-1 sequence in this case.

Lemma 13. *Suppose p is an odd prime, $p \equiv 5,7 \pmod{12}$, $\gamma = s : \widehat{S}_1, -3S_2$ is as in Theorem 11 and c_i and C_i are as in Definition 5. The following results hold.*

i)

$$c_i = \begin{cases} i-1, & 1 \le i \le (p+1)/2 \\ 3(i-1) \pmod p, & (p+3)/2 \le i \le p, \end{cases}$$

ii)

$$C_i = \begin{cases} 2i-3, & 3 \le i \le (p+1)/2 \\ 1, & i = (p+3)/2 \\ 3(2i-3) \pmod p, & (p+5)/2 \le i \le p+1, \end{cases}$$

iii)

$$-3(p-1)/2 \equiv [(p-1)/2+2] \pmod{p}.$$

iv) If $p \equiv 7 \pmod{12}$, *then*

a) $c_{(4p+8)/6} \equiv 1 \pmod{p}$
b) $C_{(4p+8)/6} \equiv -1 \pmod{p}$
c) $C_{(5p+7)/6} \equiv -2 \pmod{p}$
d) $C_{p+1} \equiv -3 \pmod{p}$.

v) If $p \equiv 5 \pmod{12}$, *then*

a) $c_{(4p+10)/6} \equiv 2 \pmod{p}$
b) $C_{(4p+4)/6} \equiv -5 \pmod{p}$
c) $C_{(5p+5)/6} \equiv -4 \pmod{p}$
d) $C_{p+1} \equiv -3 \pmod{p}$.

Proof: The computations are routine. Parts (iii)-(v) are useful in laying out examples of the constructions to follow.

Now restrict attention to the $p \equiv 7 \pmod{12}$ case.

Lemma 14. *Suppose p is an odd prime,* $p \equiv 7 \pmod{12}$ *and* $\gamma = s : \widehat{S}_1, -3S_2$ *is as in Theorem 11. The following results hold.*

i) $F_\gamma = \mathcal{A}_\gamma \cup \mathcal{B}_\gamma \cup \mathcal{C}_\gamma$ *where*

$$\begin{aligned}
\mathcal{A}_\gamma &= \{\{3i,(4p+8)/6-i\} : 1 \le i \le (p-1)/6\} \\
&= \{\{3,(4p+2)/6\},\{6,(4p-4)/6\},\dots,\{(p-1)/2,(p+3)/2\}\}, \\
\mathcal{B}_\gamma &= \{\{3i-1,(4p+2)/6+i\} : 1 \le i \le (p-1)/6\} \\
&= \{\{2,(4p+8)/6\},\{5,(4p+14)/6\},\dots,\{(p-3)/2,(5p+1)/6\}\}, \\
\mathcal{C}_\gamma &= \{\{3i+1,p+1-i\} : 1 \le i \le (p-1)/6\} \\
&= \{\{4,p\},\{7,p-1\},\dots,\{(p+1)/2,(5p+7)/6\}\}.
\end{aligned}$$

ii) If $\{x,y\} \in \mathcal{A}_\gamma \cup \mathcal{C}_\gamma$, *then* $c_x + c_y \equiv 0 \pmod{p}$.
If $\{x,y\} \in \mathcal{B}_\gamma$, *then* $c_x = c_y$.

iii) $F_{t_2} = \mathcal{A}_{t_2} \cup \mathcal{B}_{t_2} \cup \mathcal{C}_{t_2} \cup \mathcal{D}_{t_2}$ *where*

$$\begin{aligned}
\mathcal{A}_{t_2} &= \begin{cases} \phi, & \textit{if } p = 7 \\ \{\{3i+2,(4p+8)/6-i\}\} : 1 \le i \le (p-7)/6, & \textit{if } p > 7 \end{cases} \\
&= \{\{5,(4p+2)/6\},\{8,(4p-4)/6\},\dots,\{(p-3)/2,(p+5)/2\}\}, \\
\mathcal{B}_{t_2} &= \{\{3i+1,(4p+8)/6+i\} : 1 \le i \le (p-1)/6\} \\
&= \{\{4,(4p+14)/6\},\{7,(4p+20)/6\},\dots,\{(p+1)/2,(5p+7)/6\}\}, \\
\mathcal{C}_{t_2} &= \{\{3i,p+2-i\} : 1 \le i \le (p-1)/6\} \\
&= \{\{3,p+1\},\{6,p\},\dots,\{(p-1)/2,(5p+13)/6\}\}, \\
\mathcal{D}_{t_2} &= \{\{(p+3)/2,(4p+8)/6\}\}.
\end{aligned}$$

iv) *If* $\{x, y\} \in \mathcal{A}_{t_2} \cup \mathcal{C}_{t_2} \cup \mathcal{D}_{t_2}$, *then* $C_x + C_y \equiv 0 \pmod{p}$.
If $\{x, y\} \in \mathcal{B}_{t_2}$, *then* $C_x = C_y$.

Proof: The computations are routine.

The general plan is to show that the 2/3 Rule and the Disagreement Rule severely restrict the number of possible 0-1 sequences compatible with γ. After that is accomplished, it is not hard to decide what happens in the few cases that remain.

It will be useful to establish a new notation as follows. Suppose a value is chosen for $\sum_{p+1}$ in row τ_2. By disagreement, $\sum_3 = (\sum_{p+1} + 1) \pmod{2}$ since $\{3, p+1\} \in \mathcal{C}_{t_2}$. Denote this by

$$\overbrace{p+1 \rightarrow 3}.$$

The bracket above means one is working with the upper (τ_2) row and that a value at $\sum_{p+1}$ forces the other value at $\sum_3$ by disagreement. Recall that $\sigma_1 = 0$ and $\sigma_{p+1} = 1$. If $\sum_{p+1}$ and σ_{p+1} are known, the 2/3 Rule gives σ_p. Then, by disagreement, σ_p forces σ_4 since $\{4, p\} \in \mathcal{C}_\gamma$. Denote this by

$$\underbrace{p \rightarrow 4}.$$

The bracket below means one is working with the lower (σ) row and that a value at σ_p forces the other value at σ_4 by disagreement. Schematically, then, the *short path* has diagram

$$\begin{array}{ccc} \overbrace{p+1 \rightarrow 3} & & \\ & \searrow & \\ & & \underbrace{p \rightarrow 4} \end{array}$$

where the arrow with no corresponding bracket implies that the 2/3 Rule was used.

Now choose a value for σ_2. This will turn out to force all other values in the proposed compatible 0-1 sequence σ. There are two parts to the *long path* that arises. The *beginning* is, in the notion established,

$$\begin{array}{ccccc} \underbrace{2 \rightarrow (4p+8)/6} & & & & \overbrace{(4p+8)/6 \rightarrow (p+3)/2}. \\ & \searrow & & \nearrow & \\ & & \underbrace{3 \rightarrow (4p+2)/6} & & \end{array}$$

Notice that the pairs used so far are the first pairs of $\mathcal{A}_\gamma$, $\mathcal{B}_\gamma$, $\mathcal{C}_\gamma$ and $\mathcal{C}_{t_2}$ and the only pair in $\mathcal{D}_{t_2}$.

If $p > 7$ continue by noting that σ_3 and σ_4 give $\sum_4$ by the 2/3 Rule.

$$\begin{aligned} &\overbrace{4 \to (4p+14)/6} \to \underbrace{(4p+14)/6 \to 5} \to \overbrace{5 \to (4p+2)/6} \\ &\to \underbrace{(4p-4)/6 \to 6} \to \overbrace{6 \to p} \to \underbrace{p-1 \to 7} \end{aligned} \tag{5}$$

The bracketed pairs are the first unused pairs in $\mathcal{B}_{t_2}$, $\mathcal{B}_\gamma$, $\mathcal{A}_{t_2}$, $\mathcal{A}_\gamma$, $\mathcal{C}_{t_2}$ and $\mathcal{C}_\gamma$ respectively. They all arise via disagreement. The unbracketed consecutive pairs all arise via the 2/3 Rule. A basic observation is that this process iterates. The n^{th} iteration of (5) is seen to be

$$\begin{aligned} &\overbrace{3n+1 \to [4p+14+6(n-1)]/6} \to \underbrace{[4p+14+6(n-1)]/6 \to 3n+2} \\ &\to \overbrace{3n+2 \to [4p+2-6(n-1)/6} \to \underbrace{[4p-4-6(n-1)]/6 \to 3n+3} \\ &\to \overbrace{3n+3 \to p-(n-1)} \to \underbrace{p-n \to 3n+4} \end{aligned} \tag{6}$$

The bracketed pairs of the n^{th} iteration are the first unused elements of $\mathcal{B}_{t_2}$, $\mathcal{B}_\gamma$, $\mathcal{A}_{t_2}$, $\mathcal{A}_\gamma$, $\mathcal{C}_{t_2}$ and $\mathcal{C}_\gamma$ respectively.

Now F_γ has $(p-1)/2$ pairs and is partitioned into three subsets $\mathcal{A}_\gamma$, $\mathcal{B}_\gamma$ and $\mathcal{C}_\gamma$, all with $(p-1)/6$ pairs. The short path has one pair in F_γ, the beginning of the long path has two pairs in F_γ and each iteration of the long path has three pairs in F_γ. It follows that $(p-7)/6$ iterations will completely determine σ. Note that since $p \equiv 7 \pmod{12}$, $(p-7)/6$ is even.

Lemma 15. *Suppose* p *is an odd prime,* $p \equiv 7 \pmod{12}$ *and* $\gamma = s : \widehat{S}_1, -3S_2$ *is as in Theorem 11. There are exactly four possibilities for a 0-1 sequence* σ *compatible with* γ.

Proof: $\sum_{p+1}$, can be either 0 or 1 and σ_2 can be either 0 or 1. As shown above, once these choices are made everything else is forced.

Lemma 15 does not say that there always is a compatible 0-1 sequence. In fact, conflicts between the two rules may arise at the end of the long path. An analysis of the iteration process shows that the values of five σ-row positions determine what happens for the entire iteration. The *controlling positions* at the start of the first iteration are (in order)

$$(P_1, P_2, P_3, P_4, P_5) = (3, 4, (4p+2)/6, (4p+8)/6, p).$$

After two iterations, the new controlling position P_1 is the old P_1 plus 6. In general

$$\begin{array}{lll} P_1 \leftarrow P_1 + 6 & P_3 \leftarrow P_3 - 2 & P_5 \leftarrow P_5 - 2 \\ P_2 \leftarrow P_2 + 6 & P_4 \leftarrow P_4 + 2 & \end{array}$$

This process also repeats with every two iterations of the long path.

Let the initial value of controlling position P_i be denoted IV_i and the final value after $(p-7)/6$ iterations be denoted FV_i.

Lemma 16. *Suppose p is an odd prime, $p \equiv 7 \pmod{12}$ and $\gamma = s : \widehat{S}_1, -3S_2$ is as in Theorem 11. Pick a value for $\sum_{p+1}$ and for σ_2 and compute the associated σ-row and τ_2-row using the short path and long path. Then (with arithmetic in Z_2), σ is a compatible 0-1 sequence for γ iff*

i) $FV_2 + FV_3 \neq IV_3 + IV_4 = \sigma_{(4p+2)/6} + \sigma_{(4p+8)/6}$

ii) $FV_1 + FV_2 \neq FV_4 + FV_5$.

Proof: Condition (i) guarantees no conflict in the entries for the F_{t_2} position pair $\{(p+3)/2, (4p+8)/6\}$ and condition (ii) prevents a conflict in entries for the F_{t_2} position pair $\{(p+1)/2, (5p+7)/6\}$.

It is clear that as p gets larger and more iterations are required for the long path, the ordered 5-tuple $(FV_1, FV_2, FV_3, FV_4, FV_5)$ must cycle since only 32 possibilities exist. Fortunately the cycle is always of length 2 (i.e., 4 basic iterations).

Lemma 17. *Suppose p is an odd prime, $p \equiv 7 \pmod{12}$ and $\gamma = s : \widehat{S}_1, -3S_2$ is as in Theorem 11. Consider the four possibilities for the ordered pair $(\sum_{p+1}, \sigma_2)$.*

i) $(\sum_{p+1}, \sigma_2) = (0,0)$. *Then for* $n \geq 0$

a) *after $4n$ iterations,* $(FV_1, \ldots, FV_5) = (1,0,0,1,1)$,

b) *after $2+4n$ iterations,* $(FV_1, \ldots, FV_5) = (0,0,1,1,1)$.

ii) $(\sum_{p+1}, \sigma_2) = (0,1)$. *Then for* $n \geq 0$

a) *after $4n$ iterations* $(FV_1, \ldots, FV_5) = (0,0,1,0,1)$,

b) *after $2+4n$ iterations* $(FV_1, \ldots, FV_5) = (0,1,1,1,0)$.

iii) $(\sum_{p+1}, \sigma_2) = (1,0)$. *Then for* $n \geq 0$

a) *after $4n$ iterations* $(FV_1, \ldots, FV_5) = (0,1,1,1,0)$,

b) *after $2+4n$ iterations* $(FV_1, \ldots, FV_5) = (0,0,1,0,1)$.

iv) $(\sum_{p+1}, \sigma_2) = (1,1)$. *Then for* $n \geq 0$

a) *after $4n$ iterations* $(FV_1, \ldots, FV_5) = (1,1,0,0,0)$,

b) *after $2+4n$ iterations* $(FV_1, \ldots, FV_5) = (0,1,1,0,0)$.

Proof: The computations are straightforward.

Theorem 18. *Suppose p is an odd prime, $p \equiv 7 \pmod{12}$ and $\gamma = s : \widehat{S}_1, -3S_2$ is as in Theorem 11. Then γ has exactly one 0-1 sequence σ that is compatible with γ and Z_{2p} has a symmetric T_2-sequencing.*

Proof: Suppose first that $p \equiv 7 \pmod{24}$. Then $4n$ iterations of the long path are required to compute the σ-row ($n = 0$ if $p = 7$) so that $IV_j = FV_j$ in this situation. Apply Lemma 16 to the four (a) cases of Lemma 17 and only the $(0,0)$ case survives. If $p = 7$, the symmetric T_2-sequencing of Z_{14} that arises is equivalent (in the sense of [10]) to the unique example found in [10].

Suppose $p \equiv 19 \pmod{24}$. Then $2 + 4n$ iterations of the long path are required to compute the σ-row. Apply Lemma 16 to the four (b) cases of Lemma 17 (note that IV_3 and IV_4 come from the corresponding (a) cases) and only the $(1, 0)$ case survives. This completes the proof.

It is now possible to answer the question of [10] about the existence of an infinite class of $n \times n$ Tuscan-2 squares such that $n + 1$ is composite.

Remark 19. *If p is an odd prime, $p \equiv 7 \pmod{12}$, then $2p + 1$ is composite.*

Proof: Clearly $2p + 1 = 12n + 3 = 3(4n + 1)$.

A consequence of Dirichlet's Theorem is that there are infinitely many primes p such that $p \equiv 7 \pmod{12}$.

Before going on to the $p \equiv 5 \pmod{12}$ case, the reader might like to verify the following computations for $p = 19$.

$\gamma = s : \widehat{S}_1, -3S_2 = \widehat{S}_1, 16S_2$

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
τ_2:			3,	5,	7,	9,	11,	13,	15,	17,	1,	6,	12,	18,	5,	11,	17,	4,	10,	16
γ:	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	11,	14,	17,	1,	4,	7,	10,	13,	16	
δ:	0,	1,	3,	6,	10,	15,	2,	9,	17,	7,	18,	13,	11,	12,	16,	4,	14,	8,	5	

$$
\begin{aligned}
F_{t_2} &= \mathcal{A}_{t_2} \cup \mathcal{B}_{t_2} \cup \mathcal{C}_{t_2} \cup \mathcal{D}_{t_2} \\
&= \{\{5,13\},\{8,12\}\} \cup \{\{4,15\},\{7,16\},\{10,17\}\} \\
&\quad \cup \{\{3,20\},\{6,19\},\{9,18\}\} \cup \{\{11,14\}\} \\
F_{\gamma} &= \mathcal{A}_{\gamma} \cup \mathcal{B}_{\gamma} \cup \mathcal{C}_{\gamma} \\
&= \{\{3,13\},\{6,12\},\{9,11\}\} \cup \{\{2,14\},\{5,15\},\{8,16\}\} \\
&\quad \cup \{\{4,19\},\{7,18\},\{10,17\}\}
\end{aligned}
$$

short path:

$$
\begin{array}{ccc}
\overbrace{20 \to 3} & & \\
& \searrow & \\
& & \underbrace{19 \to 4}
\end{array}
$$

beginning of long path:

$$
\begin{array}{ccccc}
\underbrace{2 \to 14} & & & & \overbrace{14 \to 11} \\
& \searrow & & \nearrow & \\
& & \underbrace{3 \to 13} & &
\end{array}
$$

first iteration: $\overbrace{4 \rightarrow 15} \rightarrow \underbrace{15 \rightarrow 5} \rightarrow \overbrace{5 \rightarrow 13} \rightarrow \underbrace{12 \rightarrow 6} \rightarrow \overbrace{6 \rightarrow 19} \rightarrow \underbrace{18 \rightarrow 7}$

last iteration: $\overbrace{7 \rightarrow 16} \rightarrow \underbrace{16 \rightarrow 8} \rightarrow \overbrace{8 \rightarrow 12} \rightarrow \underbrace{11 \rightarrow 9} \rightarrow \overbrace{9 \rightarrow 18} \rightarrow \underbrace{17 \rightarrow 10}$

Choose $(\sum_{20}, \sigma_2) = (1, 0)$.

Position:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
τ_2:			0	1	1	0	0	1	1	0	1	0	0	0	0	1	1	0	1	1
σ:	0	0	0	1	0	0	0	1	0	0	1	1	1	1	1	0	1	1	0	1

Finally γ and σ give α on Z_{38}.

T_2			22,	5,	7,	28,	30,	13,	15,	36,	1,	6,	12,	18,	24,	11,	17,	4,	29,	35
α:	0,	20,	2,	3,	4,	24,	6,	7,	8,	28,	11,	33,	17,	1,	23,	26,	29,	13,	16,	19
β:	0,	20,	22,	25,	29,	15,	21,	28,	36,	26,	37,	32,	11,	12,	35,	23,	14,	27,	5,	24
T_2:		3,	9,	34,	21,	27,	14,	20,	26,	32,	37,	2,	23,	25,	8,	10,	31,	33,	16	
α:		22	25,	9,	12,	15,	37,	21,	5,	27,	10,	30,	31,	32,	14,	34,	35,	36,	18	
β:		8	33,	4,	16,	31,	30,	13,	18,	7,	17,	9,	2,	34,	10,	6,	3,	1,	19	

By Theorem 3, the symmetric T_2-sequencing α generates a 2-complete 38×38 Latin square.

Procedures in the case $p \equiv 5 \pmod{12}$ are similar to those just described for $p \equiv 7 \pmod{12}$.

Lemma 20. *Suppose $p > 5$ is an odd prime, $p \equiv 5 \pmod{12}$ and $\gamma = s : \widehat{S}_1, -3S_2$ is as in Theorem 11. The following results hold.*

i) $F_\gamma = A_\gamma \cup B_\gamma \cup C_\gamma$ *where*

$$\begin{aligned} A_\gamma &= \{\{3i, (4p+4)/6 + i\} : 1 \leq i \leq (p+1)/6\} \\ &= \{\{3, (4p+10)/6\}, \{6, (4p+16)/6\}, \ldots, \{(p+1)/2, (5p+5)/6\}\}, \\ B_\gamma &= \{\{3i-1, (4p+10)/6 - i\} : 1 \leq i \leq (p+1)/6\} \\ &= \{\{2, (4p+4)/6\}, \{5, (4p-2)/6\}, \ldots, \{(p-1)/2, (p+3)/2\}\}, \\ C_\gamma &= \{\{3i+1, p+1-i\} : 1 \leq i \leq (p-5)/6\} \\ &= \{\{4, p\}, \{7, p-1\}, \ldots, \{(p-3)/2, (5p+11)/6\}\}. \end{aligned}$$

ii) If $\{x, y\} \in B_\gamma \cup C_\gamma$, *then* $c_x + c_y \equiv 0 \pmod{p}$.
If $\{x, y\} \in A_\gamma$, *then* $c_x = c_y$.

iii) $F_{t_2} = \mathcal{A}_{t_2} \cup \mathcal{B}_{t_2} \cup \mathcal{C}_{t_2} \cup \mathcal{D}_{t_2}$ *where*

$$\begin{aligned}
\mathcal{A}_{t_2} &= \{\{3i+2, (4p+10)/6+i\} : 1 \le i \le (p-5)/6\} \\
&= \{\{5, (4p+16)/6\}, \{8, (4p+22)/6\}, \ldots, \{(p-1)/2, (5p+5)/6\}\}, \\
\mathcal{B}_{t_2} &= \{\{3i+1, (4p+10)/6 - i\} : 1 \le i \le (p-5)/6\} \\
&= \{\{4, (4p+4)/6\}, \{7, (4p-2)/6\}, \ldots, \{(p-3)/2, (p+5)/2\}\}, \\
\mathcal{C}_{t_2} &= \{\{3i, p+2-i\} : 1 \le i \le (p+1)/6\} \\
&= \{\{3, p+1\}, \{6, p\}, \ldots, \{(p+1)/2, (5p+11)/6\}\}, \\
\mathcal{D}_{t_2} &= \{\{(p+3)/2, (4p+10)/6\}\}.
\end{aligned}$$

iv) If $\{x, y\} \in \mathcal{B}_{t_2} \cup \mathcal{C}_{t_2}$, *then* $C_x + C_y \equiv 0 \pmod p$.
If $\{x, y\} \in \mathcal{A}_{t_2} \cup \mathcal{D}_{t_2}$, *then* $C_x = C_y$.

Proof: The computations are routine.

With the same conventions as in the $p \equiv 7 \pmod{12}$ case the short path has the same diagram

$$\begin{array}{ccc}
\overbrace{p+1 \to 3} & & \\
& \searrow & \\
& & \underbrace{p \to 4}
\end{array}$$

The beginning of the long path has the diagram

$$\begin{array}{ccccc}
\underbrace{2 \to (4p+4)/6} & & & & \overbrace{(4p+10)/6 \to (p+3)/2}. \\
& \searrow & & \nearrow & \\
& & \underbrace{3 \to (4p+10)/6} & &
\end{array}$$

Note that the pairs used so far are the first pairs of $\mathcal{A}_7, \mathcal{B}_7, \mathcal{C}_7$ and $\mathcal{C}_{t_2}$ and the only pair in $\mathcal{D}_{t_2}$. Again σ_3 and σ_4 give $\sum_4$ by the 2/3 Rule. Since $p > 5$, the long path continues

$$\begin{aligned}
&\overbrace{4 \to (4p+4)/6} \to \underbrace{(4p-2)/6 \to 5} \to \overbrace{5 \to (4p+16)/6} \\
&\to \underbrace{(4p+16)/6 \to 6} \to \overbrace{6 \to p} \to \underbrace{p-1 \to 7}.
\end{aligned} \tag{7}$$

As before, the bracketed pairs are the first unused pairs of $\mathcal{B}_{t_2}$, $\mathcal{B}_7$, $\mathcal{A}_{t_2}$, $\mathcal{A}_7$, $\mathcal{C}_{t_2}$ and $\mathcal{C}_7$ respectively and this process iterates. The n^{th} iteration is seen to be

$$\begin{aligned}
&\overbrace{3n+1 \to [(4p+4) - 6(n-1)]/6} \to \underbrace{[(4p-2) - 6(n-1)]/6 \to 3n+2} \\
&\to \overbrace{3n+2 \to [(4p+16) + 6(n-1)]/6} \to \underbrace{[(4p+16) + 6(n-1)]/6 \to 3n+3} \\
&\to \overbrace{3n+3 \to p-(n-1)} \to \underbrace{p-n \to 3n+4}.
\end{aligned} \tag{8}$$

The bracketed pairs of the n^{th} iteration are the first unused pairs of $\mathcal{B}_{t_2}$, $\mathcal{B}_\gamma$, $\mathcal{A}_{t_2}$, $\mathcal{A}_\gamma$, $\mathcal{C}_{t_2}$ and $\mathcal{C}_\gamma$ respectively. This time the cardinality of $\mathcal{C}_\gamma$ is one less than that of $\mathcal{A}_\gamma$ and $\mathcal{B}_\gamma$. This means that σ will be completely determined by $(p-5)/6$ iterations with the additional stipulation that one omits the last pair of the last iteration. For the record, the last iteration is

$$\begin{aligned} &\overbrace{(p-3)/2 \to (p+5)/2} \to \underbrace{(p+3)/2 \to (p-1)/2} \\ &\to \overbrace{(p-1)/2 \to (5p+5)/6} \to \underbrace{(5p+5)/6 \to (p+1)/2} \\ &\to \overbrace{(p+1)/2 \to (5p+11)/6} \to \underbrace{(5p+5)/6 \to (p+1)/2}\,. \end{aligned} \tag{9}$$

Since $p \equiv 5 \pmod{12}$, $(p-5)/6$ is even.

Lemma 21. *Suppose $p > 5$ is an odd prime, $p \equiv 5 \pmod{12}$ and $\gamma = s : \widehat{S}_1, -3\,S_2$ is as in Theorem 11. There are exactly four possibilities for a 0-1 sequence σ compatible with γ.*

Proof: The same argument as for Lemma 15 holds.

Once again there are controlling positions in σ. At the start of the first iteration, they are

$$(P_1, P_2, P_3, P_4, P_5) = (3, 4, (4p+4)/6, (4p+10)/6, p).$$

After two iterations, the controlling positions satisfy

$$\begin{array}{lll} P_1 \leftarrow P_1 + 6 & P_3 \leftarrow P_3 - 2 & P_5 \leftarrow P_5 - 2 \\ P_2 \leftarrow P_2 + 6 & P_4 \leftarrow P_4 + 2 & \end{array}$$

exactly as in the other case. Again this process iterates. The order of entry in controlling positions during the course of an iteration is P_3, P_4, P_1, P_5, P_2. Thus, on the last iteration, P_5 and P_2 are not needed because the last pair of the last iteration is omitted. Let FP_i denote the final position P_i. Then $\{FP_1, FP_4\} \in \mathcal{F}_\gamma$ since

$$3 + [(p-5)/12] \cdot 6 = (p+1)/2$$

and

$$(4p+10)/6 + [(p-5)/12] \cdot 2 = (5p+5)/6$$

implies

$$\{FP_1, FP_4\} = \{(p+1)/2, (5p+5)/6\} \in \mathcal{A}_\gamma.$$

Again let the initial value of the controlling position P_i be denoted by IV_i and the final value after $(p-5)/6 = 2n$ iterations be denoted by FV_i.

Lemma 22. *Suppose $p > 5$ is an odd prime, $p \equiv 5 \pmod{12}$ and $\gamma = s : \widehat{S}_1, -3S_2$ is as in Theorem 11. Pick a value for $\sum_{p+1}$ and for σ_2 and compute the aasociated σ-row and τ_2-row using the short path and long path. Then (with arithmetic in Z_2), σ is a compatible 0-1 sequence for γ iff*

i) $FV_1 \neq FV_4$
ii) $FV_4 = FV_5$
iii) $FV_1 + FV_3 \neq IV_3 + IV_4$.

Proof: Note that (i) and (ii) insure no conflict will arise on the "fold back" that occurs as the last step of the last iteration. Finally, (iii) prevents a conflict in entries for the F_{t_2} position pair $\{(p+3)/2, (4p+10)/6\}$.

Again $(FV_1, FV_2, FV_3, FV_4, FV_5)$ must cycle after a certain number of iterations.

Lemma 23. *Suppose $p > 5$ is an odd prime, $p \equiv 5 \pmod{12}$ and $\gamma = s : \widehat{S}_1, -3S_2$ is as in Theorem 11. Consider the four possibilities for the ordered pair $(\sum_{p+1}, \sigma_2)$.*

i) $(\sum_{p+1}, \sigma_2) = (0,0)$. *Then for $n \geq 0$*
a) *after $4n$ iterations* $(FV_1, \ldots, FV_5) = (1,0,1,0,1)$,
b) *after $2 + 4n$ iterations* $(FV_1, \ldots, FV_5) = (0,0,1,1,1)$.

ii) $(\sum_{p+1}, \sigma_2) = (0,1)$. *Then for $n \geq 0$*
a) *after $4n$ iterations* $(FV_1, \ldots, FV_5) = (0,0,0,1,1)$,
b) *after $2 + 4n$ iterations* $(FV_1, \ldots, FV_5) = (0,1,1,1,0)$.

iii) $(\sum_{p+1}, \sigma_2) = (1,0)$. *Then for $n \geq 0$*
a) *after $4n$ iterations* $(FV_1, \ldots, FV_5) = (0,1,1,1,0)$,
b) *after $2 + 4n$ iterations* $(FV_1, \ldots, FV_5) = (0,0,0,1,1)$.

iv) $(\sum_{p+1}, \sigma_2) = (1,1)$. *Then for $n \geq 0$*
a) *after $4n$ iterations* $(FV_1, \ldots, FV_5) = (1,1,0,0,0)$,
b) *after $2 + 4n$ iterations* $(FV_1, \ldots, FV_5) = (0,1,0,1,0)$.

Proof: The computations are straightforward.

Theorem 24. *Suppose $p > 5$ is an odd prime, $p \equiv 5 \pmod{12}$ and $\gamma = s : \widehat{S}_1, -3S_2$ is as in Theorem 11. If $p \equiv 5 \pmod{24}$ then γ has exactly two 0-1 sequences σ that are compatible with γ and these give rise to inequivalent (in the sense of [10]) symmetric T_2-sequencings of Z_{2p}. If $p \equiv 17 \pmod{24}$ then γ has no compatible 0-1 sequence σ.*

Proof: Consider the case $p \equiv 17 \pmod{24}$ first. In this situation $2 + 4n$ iterations (modulo the modification on the last iteration) are required to compute the σ-row. Apply Lemma 22 to the four (b) cases of Lemma 23 (note that IV_3 and IV_4 come from the corresponding (a) cases) and all cases fail.

Suppose $p \equiv 5 \pmod{24}$. Then $4n$ iterations are required to compute the σ-row. Apply Lemma 22 to the four (a) cases of Lemma 23 and the (0,1) and (1,1) cases survive.

In order to show that the two solutions are inequivalent, it suffices to consider the first three positions of the associated γ's and σ's. Clearly

$$\gamma : 0, 1, 2, \dots$$
$$\delta : 0, 1, 3, \dots$$

in each case. It can easily be shown that the associated σ's are as follows.

Case (0,1): $\sigma : 0, 1, 0, \dots$ $\rho : 0, 1, 1, \dots$ Case (1,1): $\sigma : 0, 1, 1, \dots$ $\rho : 0, 1, 0, \dots$

When each of these cases is applied to lift γ, the associated β begins as follows.

Case (0,1): $\beta : 0, 1,$ odd Case (1,1): $\widehat{\beta} : 0, 1,$ even

Clearly there is no automorphism φ of Z_{2p} such that $\varphi[\beta] = \widehat{\beta}$.

Remark 25. *Theorem 24 can be extended to include* $p = 5$.

Proof: This is an easy hand computation. Note that $C_\gamma = \phi$ if $p = 5$. It turns out that the short path gives all of the σ-row so that only two cases exist; $\sum_6 = \{0, 1\}$. Both of these cases work and they give the only two examples [10] that exist.

Remark 26. *If p is an odd prime,* $p \equiv 5 \pmod{24}$, *then* $2p + 1$ *is composite infinitely often.*

Proof: (P.A. Leonard) Require, in addition to the hypothesis, that $p \equiv 2 \pmod{5}$. The two conditions are equivalent (by the Chinese Remainder Theorem) to the single condition $p \equiv 77 \pmod{120}$. By Dirichlet there are infinitely many such primes and in each such case, $5 \mid 2p + 1$.

Suppose G is a finite group with a unique element of order two and α is a symmetric sequencing of G/Z_2. Since α is clearly a 2-sequencing of G/Z_2, it can be lifted to a collection of symmetric sequencings of G. In certain situations, the idea of doubling and redoubling symmetric sequences is very useful. That is not true in the current context.

Theorem 27. *Supppose G is a finite group with a unique element Z of order 2 and*

$$\gamma : e, c_2, c_3, \dots, c_n$$

is a 2-sequencing of G/Z_2. *Consider the following patterns.*

i) $c_i, c_{i+1}, c_{i+2} = \left\{ \begin{matrix} UZ \\ U \end{matrix} \right\}, \left\{ \begin{matrix} \widehat{Z}Z \\ \widehat{Z} \end{matrix} \right\}, \left\{ \begin{matrix} U^{-1}Z \\ U^{-1} \end{matrix} \right\}$, *where* $\widehat{Z}^2 = Z$, *ii)* $c_i, c_{i+1}, \ldots, c_j, c_{j+1} = \left\{\begin{matrix} UZ \\ U \end{matrix}\right\}, \left\{\begin{matrix} VZ \\ V \end{matrix}\right\}, \ldots, \left\{\begin{matrix} V^{-1}Z \\ V^{-1} \end{matrix}\right\} \left\{\begin{matrix} U^{-1}Z \\ U^{-1} \end{matrix}\right\},$

iii) $c_i, c_{i+1}, \ldots, c_j, c_{j+1} = \left\{\begin{matrix} UZ \\ U \end{matrix}\right\}, \left\{\begin{matrix} VZ \\ V \end{matrix}\right\}, \ldots, \left\{\begin{matrix} UZ \\ U \end{matrix}\right\}, \left\{\begin{matrix} VZ \\ V \end{matrix}\right\},$

iv) $c_i, c_{i+1}, \ldots, c_j, c_{j+1} = \left\{\begin{matrix} UZ \\ U \end{matrix}\right\}, \left\{\begin{matrix} VZ \\ V \end{matrix}\right\}, \ldots, \left\{\begin{matrix} VZ \\ V \end{matrix}\right\}, \left\{\begin{matrix} UZ \\ U \end{matrix}\right\}.$ *If* γ *has any of the patterns (i), (ii), or (iii) or* G *is Abelian and* γ *has pattern (iv), then* γ *cannot be lifted to a symmetric* T_2*-sequencing of* G.

Proof: The argument is based on the basic properties of possible lifts (see Lemma 3 and the proof of Theorem 4 in [3]) and is very simple. Note that (iv) gives an alternate way of doing Theorem 12.

Corollary 28. *If* G *is a finite group with a unique element of order 2 and* σ *is a symmetric* T_2*-sequencing of* G/Z_2*, then* α *cannot be lifted to a symmetric* T_2*-sequencing of* G.

Proof: Use either (i) or (ii) of the preceding result.

References

1. B. A. Anderson, *Sequencings and Starters*, Pacific J. of Math. **64** (1976), 17–24.
2. B. A. Anderson, *Some Perfect 1-Factorizations*, Proc. of Seventh Southeastern Conference on Combinatorics, Graph Theory and Computing (1976), 79–91.
3. B. A. Anderson, *Sequencings of Dicyclic Groups*, Ars Combinatoria **23** (1987), 131–142.
4. B. A. Anderson, *A Fast Method for Sequencing Low Order Non-Abelian Groups*, Annals of Discrete Math **34** (1987), 27–42.
5. B. A. Anderson, S_5, A_5 *and All Non-Abelian Groups of Order 32 are Sequenceable*, Congressus Numerantium **58** (1987), 53–68.
6. T. M. Apostol, "Introduction to Analytic Number Theory", Springer-Verlag, 1976.
7. R. A. Bailey, *Quasi-Complete Latin Squares: Construction and Randomization*, J. of Royal Stat. Soc. **B46** (1984), 323–334.
8. J. Dénes and A. D. Keedwell, "Latin Squares and Their Applications", Academic Press, 1974.
9. T. Etzion, S. W. Golomb and H. Taylor, *Tuscan-K Squares*, Advances in Applied Math **10** (1989), 164–174.
10. S. W. Golomb, T. Etzion and H. Taylor, *Polygonal Path Constructions for Tuscan-K Squares*, Ars Combinatoria (to appear).
11. S. W. Golomb and H. Taylor, *Tuscan Squares—A New Family of Combinatorial Designs*, Ars Combinatoria **20B** (1985), 115–132.
12. B. Gordon, *Sequences in Groups with Distinct Partial Products*, Pacific J. of Math. **11** (1961), 1309–1313.
13. A. D. Keedwell, *On the Sequenceability of Non-Abelian Groups of Order* pq, Discrete Math. **37** (1981), 203–216.
14. M. Suzuki, "Group Theory II", Springer-Verlag, 1986.
15. T. W. Tilson, *A Hamiltonian Decomposition of* K_{2m}^*, $2m \geq 8$, J. Comb. Theory **B29** (1980), 68–74.