

Cyclic Structures with Lag-Time Generators

Rachel Betz, Sandrah Eckel, Peter Pappas, and Jennifer Uyanik

For Don Passman on the occasion of his 65th birthday

ABSTRACT. The aim of this paper is to introduce the theory of lag-time sequences. The results lead us to a nice class of torus knots and also provide us with generalizations of classical results from number theory and group theory.

Introduction

The notion of a **lag-time sequence** is motivated by a particular form of the Chinese Remainder Theorem: *If m, n are integers ≥ 1 and*

$$I_m \times I_n = \{0, \dots, m-1\} \times \{0, \dots, n-1\},$$

then starting at $(0, 0)$ and repeatedly incrementing by $(1, 1)$ modulo $m\mathbf{Z} \times n\mathbf{Z}$ yields all ordered pairs of $I_m \times I_n$ if and only if $\gcd(m, n) = 1$.

This viewpoint is suggestive. For suppose we begin with $(0, 0)$ but allow the coordinates to increment by 1 at **different rates**. Then it is possible to obtain all ordered pairs of $I_m \times I_n$ without $\gcd(m, n) = 1$.

2000 *Mathematics Subject Classification*. Primary: 11A05, 11B50, 15A36; Secondary: 57M25, 57M27.

Key words and phrases. Lag-time sequences, lag-time matrices, sequences in groups, torus knots.

The first, second, and fourth authors were partially supported by a grant from the Undergraduate Research Summer Institute at Vassar College.

For instance given $m = n = 3$ we can generate all 9 ordered pairs simply by writing in array form (ordered lexicographically)

$$\begin{array}{l} (0, 0), (0, 1), (0, 2) \\ (1, 0), (1, 1), (1, 2) \\ (2, 0), (2, 1), (2, 2) \\ (0, 0), \dots \end{array}$$

where the first coordinate increments by 1 mod 3 only after the second coordinate has incremented 3 times by 1 mod 3. Were we to continue this list under the rule that the first coordinate changes by 1 mod 3 only after 3 increments of the second coordinate by 1 mod 3, we would arrive at an infinite sequence of terms from $I_3 \times I_3$ which repeats for the first time at the starting point $(0, 0)$ and which continues to repeat over the terms of the sequence already formed. This depicts a sequence of **lag-time** $l = 3$ that is **cyclic**.

In contrast, if we start at $(0, 0) \in I_2 \times I_3$ and generate modulo $2\mathbf{Z} \times 3\mathbf{Z}$ a sequence where each coordinate increments by 1 and where the first coordinate has lag-time $l = 2$, we then obtain the sequence as an array

$$\begin{array}{l} (0, 0), (0, 1), (1, 2) \\ (1, 0), (0, 1), (0, 2) \\ (1, 0), (1, 1), (0, 2) \\ (0, 0), (1, 1), (1, 2) \\ (0, 0), \dots \end{array}$$

or more simply as the **lag-time matrix** $A(m, n, l) = A(2, 3, 2)$:

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ \vdots & \vdots & \end{pmatrix}.$$

The partial listing of this sequence immediately shows that a repetition occurs prior to going back to $(0, 0)$ (that is, e.g. the second and fifth terms = $(0, 1)$). Moreover continuing this sequence with lag-time 2 we find that the next term beyond the first repeat of $(0, 0)$ is $(1, 1)$ and not $(0, 1)$. This is an example of a sequence of lag-time $l = 2$ that is not cyclic, yet $\gcd(2, 3) = 1$.

Consider the lag-time sequences starting at $(0,0) \in I_2 \times I_6$ with lag-times $l = 2, 3, 5$. For $l = 2$ we obtain

$$\begin{aligned} &(0,0), (0,1), (1,2), (1,3), (0,4), (0,5) \\ &(1,0), (1,1), (0,2), (0,3), (1,4), (1,5) \\ &(0,0), \dots \end{aligned}$$

In matrix form this becomes $A(2,6,2)$:

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ \vdots & & & & & \vdots \end{pmatrix}.$$

This lag-time sequence is cyclic. Moreover we obtain all 12 ordered pairs of $I_2 \times I_6$ while $\gcd(2,6) \neq 1$.

Next consider the lag-time sequence with $l = 3$:

$$\begin{aligned} &(0,0), (0,1), (0,2), (1,3), (1,4), (1,5) \\ &(0,0), \dots \end{aligned}$$

In matrix form this becomes $A(2,6,3)$:

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ \vdots & & & & & \vdots \end{pmatrix}.$$

Although our lag-time sequence is cyclic for $l = 3$, it produces only 6 of the 12 ordered pairs of $I_2 \times I_6$.

Finally, consider the lag-time sequence with $l = 5$:

$$\begin{aligned} &(0,0), (0,1), (0,2), (0,3), (0,4), (1,5) \\ &(1,0), (1,1), (1,2), (1,3), (0,4), (0,5) \\ &(0,0), (0,1), (0,2), (1,3), (1,4), (1,5) \\ &(1,0), (1,1), (0,2), (0,3), (0,4), (0,5) \\ &(0,0), (1,1), (1,2), (1,3), (1,4), (1,5) \\ &(0,0), \dots \end{aligned}$$

In matrix form this becomes $A(2,6,5)$:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \vdots & & & & & \vdots \end{pmatrix}.$$

This lag-time sequence is not cyclic.

Note that in all preceding examples we have a cyclic lag-time sequence if and only if l divides n . As the following example illustrates, the foregoing arithmetic condition is not necessary for a lag-time sequence to be cyclic.

Consider the lag-time sequence starting at $(0, 0) \in I_6 \times I_6$ with lag-time $l = 5$:

$$\begin{aligned} &(0, 0), (0, 1), (0, 2), (0, 3), (0, 4), (1, 5) \\ &(1, 0), (1, 1), (1, 2), (1, 3), (2, 4), (2, 5) \\ &(2, 0), (2, 1), (2, 2), (3, 3), (3, 4), (3, 5) \\ &(3, 0), (3, 1), (4, 2), (4, 3), (4, 4), (4, 5) \\ &(4, 0), (5, 1), (5, 2), (5, 3), (5, 4), (5, 5) \\ &(0, 0), \dots \end{aligned}$$

In matrix form this becomes $A(6, 6, 5)$:

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 2 & 2 \\ 2 & 2 & 2 & 3 & 3 & 3 \\ 3 & 3 & 4 & 4 & 4 & 4 \\ 4 & 5 & 5 & 5 & 5 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \vdots & & & & & \vdots \end{pmatrix}.$$

The sequence is cyclic, and l does not divide n .

The paper is organized as follows. In Section 1 we set up preliminaries and in Section 2 we introduce lag-time sequences. Here we present a theorem of H. W. Lenstra Jr., giving necessary and sufficient conditions for a lag-time sequence to be cyclic (Theorem 2.3). From this we immediately derive some corollaries. In particular we give a lag-time version of the Chinese Remainder Theorem (Theorem 2.7). In order to better understand lag-time sequences, it is convenient to view them as lag-time matrices. This is done in Section 3. In Section 4 the work is technical, culminating with our Frequency Result (Theorem 4.2). Here we show that the number of times a value arises in a given column is uniformly given as a function of m , n , l . From this we immediately obtain an alternate proof of Theorem 2.3, phrased in terms of lag-time matrices (Theorem 4.3), as well as a generalization of the Chinese Remainder Theorem (Theorem 4.5). In Section 5 we then show that modulo a certain equivalence relation the values are evenly distributed (Theorem 5.5). In this way we see that a lag-time sequence is built up from subsequences modulo an equivalence relation induced from the corresponding lag-time matrix. In Section 6 we give

an example detailing the results of this paper, and in Section 7 we give concluding remarks, including a connection to torus knots.

1. Preliminaries

Throughout this paper we assume familiarity with [La] and [NST]. We denote the cardinality of a set S by $|S|$ or $\#S$. Let $n \geq 1$ be an integer. We let \mathbf{Z} denote the additive group of integers and $\mathbf{Z}/n\mathbf{Z}$ the factor group with elements $[0]_n, \dots, [n-1]_n$. If a, b are integers, not both zero, we denote their greatest common divisor as $\gcd(a, b)$. Their least common multiple is written $ab/\gcd(a, b)$. We denote by $\lfloor r \rfloor$ the greatest integer less than or equal to r and by $\lceil r \rceil$ the least integer greater than or equal to r , for any real r . If G is a group, then we write $\langle x \rangle$ for the cyclic subgroup generated by $x \in G$.

Let $(s_\alpha)_{\alpha=0}^\infty$ be a sequence of elements from some set. We say that $(s_\alpha)_{\alpha=0}^\infty$ is **fully repeating** if there exists $d > 0$ such that for each $\alpha \geq 0$, we have $s_\alpha = s_{\alpha \bmod d}$. The least such $d > 0$ is called the **order** of the fully repeating sequence. In this case we say that the sequence $(s_\alpha)_{\alpha=0}^\infty$ is fully repeating after s_{d-1} . We define $(s_\alpha)_{\alpha=0}^\infty$ to be **cyclic** if it is fully repeating and satisfies $s_\alpha \neq s_{\alpha'}$ for every α, α' such that $0 \leq \alpha < \alpha' \leq d-1$. The **order** of a cyclic sequence is that of a fully repeating sequence.

Let $S = (s_\alpha)_{\alpha=0}^\infty$ be a fully repeating sequence of order d . Then the **underlying set of terms of S** is defined to be the set $\{s_0, \dots, s_{d-1}\}$ and we observe that the underlying set of terms of S has cardinality d if and only if the sequence S is cyclic.

Further if $(s_\alpha)_{\alpha=0}^\infty$ is cyclic of order d , then the underlying set $\{s_0, \dots, s_{d-1}\}$ inherits a cyclic group structure of order d in the obvious way.

2. Lag-Time Sequences

Let m, n, l be integers with $m \geq 2, n \geq 1$ and $1 \leq l \leq n$. The **lag-time sequence** $S(m, n, l)$ is given by $(s_\alpha)_{\alpha=0}^\infty$ where

$$s_\alpha = (\lfloor \alpha/l \rfloor \bmod m, \alpha \bmod n)$$

for every $\alpha \geq 0$. If $(s_\alpha)_{\alpha=0}^\infty$ is a cyclic lag-time sequence, then we identify $(s_\alpha)_{\alpha=0}^\infty$ with its induced cyclic group, and we write $(\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z})_l$.

REMARKS. The lag-time is not well defined for the case $m = 1$, and therefore we shall always assume $m \geq 2$. Formally, we have defined only a notion of lag-time sequence in which the first coordinate is so-called lagging. This is sufficient for our purposes and the details of defining a lag-time sequence in the other coordinate are safely left to the reader.

LEMMA 2.1. *Let m, n, l be integers with $m \geq 2, n \geq 1$ and $1 \leq l \leq n$. Let $d > 0$. The following are equivalent.*

- (1) $S(m, n, l) = (s_\alpha)_{\alpha=0}^\infty$ fully repeats after s_{d-1} ;
- (2) d is a common multiple of n and lm .

PROOF. Assume (1). A straightforward argument using the definition of lag-time sequence, together with $m \geq 2$, yields $s_d = (0, 0)$ and $s_{d+l-1} = (0, l-1)$. Then

$$\left\lfloor \frac{d}{l} \right\rfloor \equiv \cdots \equiv \left\lfloor \frac{d+l-1}{l} \right\rfloor \equiv 0 \pmod{m}$$

and therefore d is a multiple of lm . Moreover

$$d \equiv 0 \pmod{n}$$

so $n|d$ and we have (1) implies (2). Conversely, if d is a common multiple of lm and n then

$$\begin{aligned} s_{dq+r} &= \left(\left\lfloor \frac{dq+r}{l} \right\rfloor \pmod{m}, (dq+r) \pmod{n} \right) \\ &= \left(\frac{dq}{l} + \left\lfloor \frac{r}{l} \right\rfloor \pmod{m}, r \pmod{n} \right) \\ &= \left(\left\lfloor \frac{r}{l} \right\rfloor \pmod{m}, r \pmod{n} \right) \\ &= s_r. \end{aligned}$$

This proves (2) implies (1). \square

PROPOSITION 2.2. *Let m, n, l be integers with $m \geq 2, n \geq 1$ and $1 \leq l \leq n$. The lag-time sequence $S(m, n, l)$ has order $nlm/\gcd(n, lm)$.*

PROOF. The order of $S(m, n, l)$ is the least $d > 0$ such that $S(m, n, l)$ is fully repeating. By the previous lemma, it follows that d is the least common multiple of n and ml , so that $d = nlm/\gcd(n, lm)$ as desired. \square

The following result was first suggested to us by H. W. Lenstra Jr. during his visit to Vassar in 2004. With his kind permission we include a version of his proof.

THEOREM 2.3 ([Le]). *Let m, n, l be integers with $m \geq 2, n \geq 1$ and $1 \leq l \leq n$. The lag-time sequence $S(m, n, l)$ is cyclic if and only if $\gcd(n, lm) \geq l$.*

PROOF. Let $\langle(1, l)\rangle$ be the cyclic subgroup of $\mathbf{Z} \times \mathbf{Z}$, generated by $(1, l)$. Let

$$G = \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

and let H be the image of $\langle(1, l)\rangle$ under the canonical homomorphism

$$\mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

Assume $S(m, n, l)$ has order d and consider the subsequence $(t, tl) \in \mathbf{Z} \times \mathbf{Z}$ consisting of the l^{th} terms starting at $(0, 0)$. By Lemma 2.1 d is the first value of α divisible by l with $s_\alpha = (0, 0)$. Therefore the order of this subsequence is d/l . Each l^{th} term of $S(m, n, l)$ is of the form (t, tl) so defines an element of $\langle(1, l)\rangle$ and conversely. Since H is a cyclic group generated by the image of $(1, l)$ it follows that $|H| = d/l$.

The underlying set of terms of $S(m, n, l)$ is therefore in bijection with

$$(0, 0) + H \cup (0, 1) + H \cup \cdots \cup (0, l-1) + H,$$

and hence this union has cardinality d if and only if $S(m, n, l)$ is cyclic. Thus $S(m, n, l)$ is cyclic if and only if, for $t = 0, \dots, l-1$, the l cosets $(0, t) + H$ are disjoint. It follows that $S(m, n, l)$ is cyclic if and only if the order of $(0, 1) + H$ in G/H is $\geq l$.

To this end we claim that the cyclic group G/H is generated by $(0, 1) + H$. Indeed, for any $(a, b) \in \mathbf{Z} \times \mathbf{Z}$, we have

$$(a, b)a(1, l) - al(0, 1) + (b - al)(0, 1),$$

so that

$$(a, b) + H = (b - al)(0, 1) + H \in \langle(0, 1) + H\rangle,$$

thereby establishing the claim.

By Proposition 2.2 the order of $S(m, n, l)$ is $d = nlm/\gcd(n, lm)$, and therefore

$$|\langle(0, 1) + H\rangle| = |G/H| = |G|/|H| = \frac{mn}{mn/\gcd(n, lm)} = \gcd(n, lm).$$

Thus $S(m, n, l)$ is cyclic if and only if $\gcd(n, lm) \geq l$. \square

REMARK. A discussion of Theorem 2.3 is included at the end of the paper including a nice proof due to the referee.

COROLLARY 2.4. *Let $n \geq 1$ and $1 \leq l \leq n$. Then $(\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z})_l$ exists.*

PROOF. This follows by Theorem 2.3. \square

COROLLARY 2.5. *If $(\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z})_l$ exists, then its cardinality is $nlm/\gcd(n, lm)$.*

PROOF. This is Proposition 2.2. \square

COROLLARY 2.6. *If $l|n$, then $(\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z})_l$ exists and has cardinality $mn/\gcd(n/l, m)$.*

PROOF. If $l|n$ then $\gcd(n, lm) = l \gcd(n/l, m) \geq l$. Therefore $(\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z})_l$ exists by Theorem 2.3. The cardinality follows by the previous result. \square

THEOREM 2.7 (Lag-Time Version of Chinese Remainder Theorem). *Let $m \geq 2$, $n \geq 1$ and $1 \leq l \leq n$. Then $(\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z})_l$ exists and has order mn if and only if $l|n$ and $\gcd(n/l, m) = 1$.*

PROOF. This follows directly from the two previous results. \square

3. Lag-Time Matrices.

Let m, n, l be integers with $m \geq 2$, $n \geq 1$, $1 \leq l \leq n$. Let $A = (a_{ij})$ be a generic matrix of indeterminates consisting of countably infinitely many rows and n columns. Order the entries of A lexicographically as:

$$a_{ij} < a_{i'j'} \text{ if and only if } i < i' \text{ or } i = i' \text{ and } j < j'.$$

With respect to this order, assign the value $0 \bmod m$ to the first l consecutive entries of A , $1 \bmod m$ to the next l consecutive entries of A , and in general given an assignment of $k \bmod m$ to l consecutive entries we assign $(k+1) \bmod m$ to the next l consecutive entries of A . The resulting matrix is called the **lag-time matrix** $A(m, n, l)$. It is clear that the foregoing definition can be formulated precisely using recursion. We denote the i^{th} row of $A(m, n, l)$ by R_i for each $i \geq 1$.

It is easy to see that the map $a_{ij} \mapsto (a_{ij}, j-1)$, sending a sequence of a_{ij} to a sequence of pairs $(a_{ij}, j-1)$ is an order-preserving bijection between $A(m, n, l)$ and $S(m, n, l)$. By Proposition 2.2 it follows that $A(m, n, l)$ is as a matrix **fully repeating** after row R_E ; that is $R_{E+1} = R_1$ with $E = lm / \gcd(n, lm)$. Moreover E is the least integer such that $R_{E+1} = R_1$. We define $A(m, n, l)$ to be **cyclic** if $a_{ij} \neq a_{i'j}$ for all $i \neq i' \leq E$ and $j = 1, \dots, n$. It then follows that $S(m, n, l)$ is cyclic if and only if $A(m, n, l)$ is cyclic.

A **lag-class** or **complete lag-class** is an ordered set of l consecutive entries of $A(m, n, l)$ with the same value modulo m . Any two lag-classes are either identical or disjoint. If Λ and Λ' are distinct lag-classes then we write $\Lambda < \Lambda'$ if $\lambda < \lambda'$ for some $\lambda \in \Lambda$ and $\lambda' \in \Lambda'$. A **partial lag-class** of a lag-class Λ is a **proper non-empty** initial or final segment of Λ . The **length** of a complete or partial lag-class is its cardinality. We shall say that the lag-class Λ **meets row** R if Λ and R have non-empty intersection. More generally given rows R_{i_1}, \dots, R_{i_k} of $A(m, n, l)$, we say that Λ **meets** $R_{i_1} \cup \dots \cup R_{i_k}$ if Λ and $R_{i_1} \cup \dots \cup R_{i_k}$ have non-empty intersection. A lag-class Λ **lies in row** R , or R **contains the lag-class** Λ , if all elements of Λ are entries of R . If Λ meets R but is not contained in R , then R **contains a partial lag-class** of

Λ . It is easy to see that if R contains a partial lag-class consisting of r elements, then these elements constitute the first r consecutive entries of R or the last r consecutive entries of R . We say that R **ends in a complete lag-class** if the final l entries of R constitute a complete lag-class. Otherwise we say that R **ends in a partial lag-class**.

If $n = lq_1 + r_1$ with $0 < r_1 < l$, then the first row R_1 of $A(m, n, l)$ contains q_1 consecutive lag-classes and ends with a partial lag-class of length r_1 . These final r_1 entries of the first row together with the first $l - r_1$ entries of the second row constitute the $(q_1 + 1)^{\text{th}}$ lag-class. Thus there are $q_1 + 1$ lag-classes meeting R_1 .

If $l|n$ then R_1 ends in a complete lag-class and therefore R_1 is the first row ending in a complete lag-class. In general we can find the first row R_s ending in a complete lag-class as follows. For R_s to exist, a straightforward argument shows that it is necessary and sufficient that the cardinality of $R_1 \cup \dots \cup R_s$ equal the least common multiple of l and n ; that is, $nl/\gcd(n, l)$. Hence since each row contains n elements it follows that

$$s = \frac{l}{\gcd(n, l)}.$$

In general a row need not end in a complete lag-class and therefore the above analysis is insufficient for providing a detailed understanding of the lag-class structure of an arbitrary row. This leads us to the following result which can be thought of as a two-sided version of Euclid's Division Theorem.

THEOREM 3.1. *For each $k \geq 1$, let q_k be the number of complete lag-classes of row R_k and r_k be the length of the partial lag-class ending row R_k (with $r_k = 0$ if the row ends in a complete lag-class). Let δ_k be 0 if $r_k = 0$ and be 1 otherwise. Then for all k we have*

$$n = (\delta_{k-1}l - r_{k-1}) + lq_k + r_k$$

(with $r_0 = 0 = \delta_0 = 0$) and

$$q_k = q_1 + \left\lfloor \frac{r_{k-1} + r_k}{l} \right\rfloor - \delta_k$$

and

$$r_k = kr_1 \bmod l.$$

PROOF. The first k rows contain kn elements, starting with some number of complete lag-classes (some of which may span two rows) and ending with a partial lag-class of length

$$r_k = kn \bmod l = kr_1 \bmod l.$$

Since row R_k starts with a partial lag-class of length $\delta_{k-1}l - r_{k-1}$ and contains q_k complete lag-classes, the first formula follows. Finally we have

$$r_k \equiv kr_1 \equiv r_{k-1} + r_1 \pmod{l},$$

so r_k is either $r_{k-1} + r_1$ (if this latter quantity is less than l) or $r_{k-1} + r_1 - l$ (otherwise). The formula for q_k now follows from

$$n = (\delta_{k-1}l - r_{k-1}) + lq_k + r_k$$

and the same equation for $k = 1$. \square

We now obtain precisely the result stated at the outset of this section. To this end we observe that

$$\frac{l}{\gcd(n, l)} = \frac{l}{\gcd(l, r_1)}.$$

COROLLARY 3.2. *Let $m \geq 2$, $n \geq 1$ and $1 \leq l \leq n$. The lag-time matrix $A(m, n, l)$ has a row that ends in a complete lag-class. The first row R_k where this occurs has $k = \frac{l}{\gcd(l, r_1)}$ and is independent of m .*

PROOF. If R_1 ends in a complete lag-class then $l|n$ so $r_1 = 0$, and therefore $\frac{l}{\gcd(l, r_1)} = 1$. If R_1 does not end in a complete lag-class, then our result follows from Theorem 3.1 and $r_k = \left(\frac{l}{\gcd(l, r_1)}\right) r_1 \pmod{l}$. \square

THEOREM 3.3. *For any integer $t \geq 1$, the following are equivalent for $A(m, n, l)$:*

- (1) *The final l terms of the t^{th} row constitute a complete lag-class;*
- (2) *l divides tr_1 ;*
- (3) *$t = u \left(\frac{l}{\gcd(l, r_1)}\right)$ for some integer $u \geq 1$.*

PROOF. (1) holds if and only if l divides tn if and only if l divides tr_1 if and only if l divides $t \gcd(l, r_1)$ if and only if there exists a u with $ul = t \gcd(l, r_1)$ if and only if (3) holds. \square

THEOREM 3.4 (Lag-Class Structure of Rows: Part I). *Let $n = lq_1 + r_1$ for some $0 \leq r_1 < l$. Let $t = u \left(\frac{l}{\gcd(l, r_1)}\right)$ for some integer $u \geq 1$ and let $1 \leq i \leq \frac{l}{\gcd(l, r_1)}$. Let $\Lambda_1 < \dots < \Lambda_v$ and $\Lambda'_1 < \dots < \Lambda'_w$ be the distinct lag-classes meeting R_{t+i} and R_i , respectively. Then $v = w$, and the association*

$$a_{(t+i), j} \mapsto a_{ij}$$

induces an order-preserving bijection of $\Lambda_j \cap R_{t+i}$ with $\Lambda'_j \cap R_i$, for every $j = 1, \dots, v$.

PROOF. Obvious. \square

THEOREM 3.5 (Lag-Class Structure of Rows: Part II). *Let $K = \frac{l}{\gcd(l, r_1)}$. The lag-class structures for any two rows R_s and $R_{s'}$ with $s \neq s'$ and $s, s' \leq K$ are different; that is, no lag-class of R_s lies precisely over any lag-class of $R_{s'}$.*

PROOF. Consider a lag-class L that meets R_s and a lag-class L' that meets $R_{s'}$. While these lag-classes may not be complete, we let L and L' refer to the portions of these lag-classes that lie in each respective row. If L and L' begin in the same column, then L lies precisely over L' and given any lag-class in R_s there exists a lag-class in $R_{s'}$ beginning and ending in the same columns. Hence the lag-class structure of R_s is identical to that of $R_{s'}$. Also, we know that each R_{s^*} ends in a partial lag-class of length $s^*r_1 \bmod l$. Now since $[r_1]_l$ generates a subgroup of order K in $\mathbf{Z}/l\mathbf{Z}$, and since $s \neq s'$ and $s, s' \leq K$, we have that $[sr_1]_l \neq [s'r_1]_l$. Thus the final (possibly partial) lag-classes in R_s and $R_{s'}$ begin in different columns and hence R_s and $R_{s'}$ have different lag-class structures. \square

4. Frequency of Values

From our remarks at the outset of Section 3, we know that the matrix $A(m, n, l)$ fully repeats after row $E = \frac{lm}{\gcd(n, lm)}$ and that $R_1 \cup \dots \cup R_E$ has precisely $\omega_E = nlm / \gcd(n, lm)$ entries. Each value occurs the same number of times. Since there are n columns and m values, one expects that on average each value occurs $\omega_E / nm = l / \gcd(n, lm)$ times per column. For suitable choices of n, m, l this average frequency is not an integer. The aim of this section is to provide a detailed analysis of the frequency of values.

Let $s, s' \in \mathbf{N}$. We say that R_s and $R_{s'}$ are **equivalent** if they have the same lag-class structures. In this case we write $R_s \equiv R_{s'}$. We also say that R_i, \dots, R_s are equivalent to $R_{i'}, \dots, R_{s'}$ if R_j is equivalent to $R_{j'}$ for all $j = i, \dots, s$ and the respective values of j' with $j' = i', \dots, s'$.

We define the **number of occurrences of** $a_{sj} \in C_j$ to be the number of values $1 \leq i \leq E$ such that $a_{ij} = a_{sj}$. We denote this number by $\mathbf{occ}(a_{sj}, j)$. Thus

$$\mathbf{occ}(a_{sj}, j) = \#\{i \mid a_{ij} = a_{sj} \text{ for } 1 \leq i \leq E\}.$$

LEMMA 4.1. *Let a_{ij} lie within the first E rows of $A(m, n, l)$. If a_{ij} is the t^{th} element of the lag-class to which it belongs, then*

$$\mathbf{occ}(a_{ij}, j) = \mathbf{occ}(a_{1t}, j).$$

In other words, if in the j^{th} column C_j the value k arises as the t^{th} element of some lag-class, then the number of occurrences of k in C_j equals the number of occurrences of 0 in the t^{th} column C_t .

PROOF. Assume that $k = a_{ij}$ arises as the t^{th} element of some lag-class. The first member of this lag-class either lies on row R_{i-1} or row R_i . In either case, starting with this first member on row R_s , we translate all subsequent elements of $A(m, n, l)$ to the left until this first member is in the first column of R_s , thereby creating a new matrix A' in which the first l entries have value k , the next l entries have value $k + 1 \pmod{m}$, and so forth. Proceeding inductively it is easy to see that the lag-class structure of the matrices A and A' are identical. In particular, the number of occurrences of the value k in the t^{th} column C'_t of A' agrees with the number of occurrences of the value 0 in the t^{th} column C_t of A . Since translation preserves the ordering of elements, it follows that the number of occurrences of k in C_j in A equals the number of occurrences 0 in C_t in A' . \square

THEOREM 4.2 (Frequency Result). *Given $A(m, n, l)$, $1 \leq k \leq m$ and $1 \leq j \leq n$, C_j contains either $\lfloor \frac{l}{\gcd(n, lm)} \rfloor$ or $\lceil \frac{l}{\gcd(n, lm)} \rceil$ entries of value k in the first E rows.*

PROOF. By the previous lemma, it suffices to show that within any two columns, the number of occurrences of 0 is either $\lfloor \frac{l}{\gcd(n, lm)} \rfloor$ or $\lceil \frac{l}{\gcd(n, lm)} \rceil$. To this end, assume we have $1 \leq j < n$. We proceed in a series of steps.

Step 1. The number of occurrences of 0 in C_j and C_{j+1} differ by at most 1.

Assume that the number of occurrences of 0 in C_j is x and in C_{j+1} is at least $x + 2$. Then among the first E rows there must exist two distinct rows each of which contain lag-classes of value $m - 1$ ending in C_j . An easy inductive argument using Theorem 3.1 shows that these rows must be identical, an impossibility. If the number of occurrences of 0 in C_{j+1} is x and in C_j is at least $x + 2$, then among the first E rows there must exist two distinct rows each of which contain lag-classes of value 0 ending in C_j , an impossibility.

Step 2. The number of occurrences of 0 in C_j and C_{j+r} differ by at most 1, for $1 \leq j < j + r \leq n$.

By Step 1, we have $r \geq 2$. Assume that the number of occurrences of 0 in C_j is x and in C_{j+r} is at least $x + 2$. Now choose j and r with r minimal such that the number of occurrences of 0 in C_j is x and in C_{j+r} is at least $x + 2$. Then by Step 1, we have $r \geq 2$. By Step

1, it follows that the number of occurrences of 0 in each of $C_{j+1}, \dots, C_{j+r-1}$ is $x + 1$, and moreover the number of occurrences of 0 in C_{j+r} is $x + 2$. Thus there exists a lag-class of value $m - 1$ ending in C_j and there exists a lag-class of value $m - 1$ ending in C_{j+r-1} . Therefore there exist lag-classes of value 0 beginning in each of C_{j+1} and in C_{j+r} . By Lemma 4.1 this implies the number of occurrences of 0 in C_{j+1} and in C_{j+r} agree with the number of occurrences of 0 in C_1 , and hence must be equal, a contradiction.

Similarly if the number of occurrences in C_{j+r} is x and in C_j is at least $x + 2$, then we may assume that the number of occurrences of 0 in C_j is $x + 2$, the number of occurrences of 0 in each of $C_{j+1}, \dots, C_{j+r-1}$ is $x + 1$, and the number of occurrences in C_{j+r} is x . Then there exist lag-classes of value 0 ending in C_j and in C_{j+r-1} . But by Lemma 4.1 this would imply that the number of occurrences of 0 in these two columns agrees with the number of occurrences of 0 in C_l , an impossibility.

Step 3. Final contradiction.

Since the average number of occurrences is $\frac{l}{\gcd(n, lm)}$, and all differences are at most 1, the result follows. \square

We now give an alternate proof of Theorem 2.3, phrased in terms of lag-time matrices, rather than lag-time sequences.

THEOREM 4.3. *Let m, n, l be integers with $m \geq 2, n \geq 1$ and $1 \leq l \leq n$. The lag-time matrix $A(m, n, l)$ is cyclic if and only if $\gcd(n, lm) \geq l$.*

PROOF. If $\gcd(n, lm) \geq l$, then $\left\lfloor \frac{l}{\gcd(n, lm)} \right\rfloor = 0$ and $\left\lceil \frac{l}{\gcd(n, lm)} \right\rceil = 1$. By Theorem 4.2, each value k occurs in each column at most once within the first E rows, and it follows that the lag-time matrix $A(m, n, l)$ is cyclic. Conversely if $\gcd(n, lm) < l$, then

$$\left\lceil \frac{l}{\gcd(n, lm)} \right\rceil > 1,$$

so some number is repeated in some column, and $A(m, n, l)$ is not cyclic. \square

THEOREM 4.4. *The underlying set of terms of the lag-time sequence $S(m, n, l)$ has cardinality $nlm / \gcd(n, lm)$ if the sequence is cyclic and mn otherwise.*

PROOF. If $A(m, n, l)$ is not cyclic then $l > \gcd(n, lm)$ so that $\left\lfloor \frac{l}{\gcd(n, lm)} \right\rfloor \geq 1$. The result now follows from Corollary 2.5 and Theorem 4.2. \square

THEOREM 4.5 (Lag-Time Version of Chinese Remainder Theorem). *Let m, n, l be integers with $m \geq 2, n \geq 1$ and $1 \leq l \leq n$. Then the underlying set of terms of the lag-time sequence $S(m, n, l)$ has cardinality mn if and only if $\gcd(n, lm) \leq l$.*

PROOF. Immediate by Theorem 4.4 □

5. Uniform Distribution of Values

We now show that, modulo a certain equivalence relation, the values are uniformly distributed.

Let Λ be a lag-class. We define $\#\Lambda$ to be the number of lag-classes up to and including Λ under the ordering of lag-classes, as in Theorem 3.4. For any $a_{ij} \in A(m, n, l)$ we write Λ_{ij} for the lag-class containing a_{ij} . The following result is obvious but necessary.

PROPOSITION 5.1 (Assignment of Values). *Let $a_{ij}, a_{sj} \in A(m, n, l)$. Then*

$$a_{ij} = (\#\Lambda_{ij} - 1) \bmod m$$

and if $s \leq i$, then

$$a_{ij} = a_{sj} + (\#\Lambda_{ij} - \#\Lambda_{sj}) \bmod m.$$

Moreover, if $a_{ij} = a_{st}$, then

$$\#\Lambda_{ij} - \#\Lambda_{st} \equiv 0 \bmod m.$$

A **block** β is a maximal number of inequivalent rows among the first E rows of the matrix $A(m, n, l)$. By Theorem 3.5 it follows that the size of any block is $K = l / \gcd(l, r_1)$. Thus β is a block if and only if the indices of its rows give a complete system of residues modulo K . In particular any K consecutive rows form a block. Let $\beta = \{i_1, \dots, i_K\}$. For any integer s define $\beta + s = \{i_1 + s \bmod E, \dots, i_K + s \bmod E\}$ where $\{1, \dots, E\}$ forms a complete residue system modulo E . Then $\beta + s$ is also a block. A block β induces a partition of the first E rows into equivalent blocks. Indeed, let $\beta = \beta_1 = \{i_1, \dots, i_K\}$. If $\beta_1 \neq \{1, \dots, E\}$, define $\beta_2 = \beta_1 + K$. Then β_1 and β_2 are disjoint equivalent blocks. Assume β_1, \dots, β_r have been defined such that $\beta_\nu = \beta_1 + \nu K$ for every ν such that $1 \leq \nu \leq r$. If the union of β_1, \dots, β_r is not all of $\{1, \dots, E\}$ then define $\beta_{r+1} = \beta_1 + rK$. In this way we form a partition $\{\beta_1, \dots, \beta_B\}$ of the first E rows into equivalent blocks. The number B of blocks formed in this partition satisfies

$$BK = E = lm / \gcd(n, lm).$$

Thus

$$B = \frac{lm / \gcd(n, lm)}{l / \gcd(l, n)} = m / \gcd(n / \gcd(n, l), m).$$

Now $n/\gcd(n, l)$ equals the number of lag-classes in the first K rows; that is, the number μ_K of lag-classes in the first K rows is

$$\mu_K = n/\gcd(n, l).$$

It therefore follows that

$$B = \# \left\langle \left[\frac{n}{\gcd(n, l)} \right]_m \right\rangle;$$

in other words B is the order of the cyclic subgroup generated by $[\mu_K]_m$ in $\mathbf{Z}/m\mathbf{Z}$.

Let s be such that $1 \leq s \leq E$. We define the **equivalence class** of s to be

$$\mathbf{eq}(s) = \{ s' \mid R_s \equiv R_{s'} \text{ for } 1 \leq s' \leq E \}.$$

It follows that

$$\#\mathbf{eq}(s) = B.$$

For each j , $1 \leq j \leq n$, we define the **value set**

$$\mathbf{v}_j(s) = \{ a_{ij} \mid i \in \mathbf{eq}(s) \}.$$

Since no two rows among the the first E rows can be identical it follows that

$$\#\mathbf{v}_j(s) = B.$$

CONVENTION. From now on we shall write $\mathbf{eq}(s, j)$ for $\mathbf{v}_j(s)$.

THEOREM 5.2. *We have either $\mathbf{eq}(s, j) = \mathbf{eq}(s', j)$ or $\mathbf{eq}(s, j) \cap \mathbf{eq}(s', j) = \emptyset$.*

PROOF. Choose a_{sj} from among the first K rows. By Proposition 5.1 we see by induction each of the B elements of $\mathbf{eq}(s, j)$ is expressible as

$$a_{sj} + \lambda(n/\gcd(n, l))$$

for some $\lambda = 1, \dots, B$. Thus

$$\mathbf{eq}(s, j) = a_{sj} + \langle [\mu_K]_m \rangle.$$

In other words, $\mathbf{eq}(s, j)$ is a coset of the cyclic group generated by $[\mu_K]$ in $\mathbf{Z}/m\mathbf{Z}$. The result now follows. \square

THEOREM 5.3. *If $a_{ij} = a_{sj}$ then $\mathbf{eq}(i, j) = \mathbf{eq}(s, j)$.*

PROOF. This is immediate by Theorem 5.2. \square

THEOREM 5.4. *Assume R_s and $R_{s'}$ are equivalent rows for some $s \neq s'$, and $1 \leq s, s' \leq E$. Assume $a_{sj} \in R_s$ and $a_{s'j} \in R_{s'}$. Then within the first E rows the number of entries in C_j of value a_{sj} equals the number of entries in C_j of value $a_{s'j}$. This common value is either*

$$\left\lfloor \frac{l}{\gcd(n, lm)} \right\rfloor \quad \text{or} \quad \left\lceil \frac{l}{\gcd(n, lm)} \right\rceil.$$

PROOF. The value a_{sj} in C_j lies only in inequivalent rows, say $s_1 < \dots < s_r \leq E$. By definition we have $\mathbf{eq}(s, j) = \mathbf{eq}(s', j)$ and by Theorem 5.3 we have $\mathbf{eq}(s_i, j) = \mathbf{eq}(s, j)$. Thus

$$\mathbf{occ}(a_{sj}, j) \leq \mathbf{occ}(a_{s'j}, j).$$

Equality follows by reversing the roles of a_{sj} and $a_{s'j}$. The second statement is Theorem 4.2. \square

THEOREM 5.5 (Uniform Distribution of Values). *Let $1 \leq s \leq E$ and let β be a block of $A(m, n, l)$. Then the number of entries in β with values in $\mathbf{eq}(s, j)$ equals the number of occurrences of a_{sj} within the first E rows. In other words,*

$$\#\{i \in \beta \mid a_{ij} \in \mathbf{eq}(s, j)\} = \mathbf{occ}(a_{sj}, j).$$

This common value is either

$$\left\lfloor \frac{l}{\gcd(n, lm)} \right\rfloor \quad \text{or} \quad \left\lceil \frac{l}{\gcd(n, lm)} \right\rceil.$$

PROOF. We identify a block β with the subscripts enumerating the rows lying in β and we view all subscripts modulo E with $\{1, \dots, E\}$ forming a complete residue system modulo E . The block β induces a partition of the first E rows by equivalent blocks $\beta = \beta_1, \dots, \beta_B$. Let y = the number of entries in β_1 with values in $\mathbf{eq}(s, j)$. Assume $i \in \beta_1$ and $a_{ij} \in \mathbf{eq}(s, j)$. Then

$$\mathbf{eq}(s, j) = \{a_{ij}, a_{i+K, j}, \dots, a_{i+\nu K, j}, \dots, a_{i+BK, j}\}$$

with

$$a_{i+\nu K, j} \in \beta_\nu.$$

By Theorems 5.3 and 5.4 we have $\mathbf{eq}(i, j) = \mathbf{eq}(s, j)$ and so each block β_ν has y entries with values in $\mathbf{eq}(s, j)$. Overall, therefore, there are exactly yB entries with value in $\mathbf{eq}(s, j)$ within the first E rows.

On the other hand, by Theorem 5.4, each entry of $\mathbf{eq}(s, j)$ occurs x times within the first E rows. That is, if $a_{s'j} \in \mathbf{eq}(s, j)$, then $\mathbf{occ}(a_{s'j}, j) = \mathbf{occ}(a_{sj}, j)$. Thus, overall there are exactly xB entries with value in $\mathbf{eq}(s, j)$ within the first E rows. Therefore $x = y$. \square

REMARK. A lag-time matrix $A(m, n, l)$ is cyclic if and only if

$$\left\lceil \frac{l}{\gcd(n, lm)} \right\rceil = 1.$$

Moreover, by the preceding, if $A(m, n, l)$ is not cyclic then every value occurs in every column. In either instance these values are uniformly distributed modulo the equivalence of Theorem 5.5.

6. Example

Consider the lag-time sequence $S(6, 10, 7)$. Then $m = 6$, $n = 10$, and $l = 7$ so that

$$\gcd(n, lm) = \gcd(10, 42) = 2 < 7 = l.$$

By Theorem 2.3 this sequence is non-cyclic. Consider the non-cyclic matrix $A(6, 10, 7)$:

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} \\ \mathbf{2} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{4} \\ \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} \\ \mathbf{5} & \mathbf{5} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} \\ \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} \\ - & - & - & - & - & - & - & - & - & - & - \\ \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} \\ \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{2} \\ \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} \\ \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{5} \\ \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ - & - & - & - & - & - & - & - & - & - & - \\ \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} \\ \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} \\ \mathbf{4} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{3} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{4} \\ \mathbf{4} & \mathbf{4} & \mathbf{4} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} & \mathbf{5} \\ & & & & & & & & & & \vdots \end{pmatrix}.$$

We have $E = lm/\gcd(n, lm) = 21$ and $l/\gcd(n, lm) = 7/2$. By inspection, the number of occurrences of a value k in any column is

either

$$3 = \left\lfloor \frac{l}{\gcd(n, lm)} \right\rfloor$$

or

$$4 = \left\lceil \frac{l}{\gcd(n, lm)} \right\rceil.$$

This is the Frequency Result, Theorem 4.2.

Observe that $K = l / \gcd(l, r_1) = 7$, and that the first 7 rows have different lag-class structures. These 7 rows yield a block β_1 . The next 7 rows constitute a second block β_2 , and the the remaining 7 rows a third block β_3 . Hence $B=3$, so any equivalence class consists of 3 elements.

For example, rows R_1, R_8, R_{15} are equivalent and $\mathbf{eq}(1, 1) = \{0, 4, 2\}$. In the first column, the value 0 occurs 4 times; the other two values, 4 and 2, also occur 4 times. This is Theorem 5.4.

Finally consider rows $R_1, R_2, R_3, R_{11}, R_{12}, R_{13}, R_{21}$. These form a block

$$\beta = \{1, 2, 3, 11, 12, 13, 21\}.$$

In the first column, the values are, respectively,

$$0, 1, 2, 2, 3, 5, 4.$$

In this list, the values 1, 3, 5 are equivalent and occur only once for a total of $3 = \mathbf{occ}(a_{21}, 1)$ times, whereas the equivalent values 0, 2, 4 occur a total of $4 = \mathbf{occ}(a_{11}, 1)$ times. This is the Uniform Distribution of Values, Theorem 5.5.

7. Concluding Remarks

Several proofs of Theorem 2.3 now exist, each arising from different viewpoints. The original proof of H. W. Lenstra Jr. is decidedly group theoretic and the construction of the subgroup H allows one to give necessary and sufficient conditions for the underlying set of terms of $S(m, n, l)$ to be a subgroup of $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ (see [FLP]). On the other hand Theorem 2.3 follows easily from our Frequency Result (Theorem 4.2). By far the shortest proof of Theorem 2.3 is due to the referee, whom we thank for giving us permission to include the proof below. The original version of our paper did not contain Lenstra's proof, and therefore the referee's proof was found independently.

PROOF OF THEOREM 2.3 BY THE REFEREE. (Sketch.) Consider the terms s_k with k a multiple of l ; these are $(0, 0)$, $(1, l \bmod n)$, $(2 \bmod m, 2l \bmod n)$, and so forth. The first term after the initial $(0, 0)$ to have

first coordinate 0 will be $(m \bmod m, ml \bmod n) = (0, ml \bmod n)$. The terms of this subsequence with first coordinate 0 will be

$$(0, 0), (0, ml \bmod n), (0, 2ml \bmod n), \dots$$

until we get the first term $(0, cml \bmod n)$ with n dividing cml (with c positive), when the sequence starts repeating. (And the original lag-time sequence will start repeating at the corresponding point.) The second coordinates occurring here, which are the multiples of ml , taken modulo n , are the same as the multiples of $d = \gcd(ml, n)$, taken modulo n .

So the terms of the subsequence with first coordinate 0 are

$$(0, 0), (0, d), \dots, (0, n - d)$$

and the terms of the original lag-time sequence with initial coordinate 0 are

$$(0, 0), \dots, (0, l - 1), (0, d), \dots, (0, d + l - 1), \dots, \\ (0, n - d), \dots, (0, n - d + l - 1).$$

An inductive argument shows that the lag-time sequence is cyclic if and only if these terms are all distinct, which happens if and only if l is at most d . That is, the lag-time sequence is cyclic if and only if we have $l \leq \gcd(n, lm)$.

TORUS KNOTS. It is of some interest to observe that simply joining consecutive elements of a lag-time sequence $S(m, n, l)$ (which lie in $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, thought of as the lattice points in a real torus) gives a torus path directly. It is then easy to see that $S(m, n, l)$ is cyclic if and only if its corresponding path is a torus knot, and in this case the lag-time sequence $S(m, n, l)$ determines an $\left(E, \frac{n}{\gcd(n, lm)}\right)$ -torus knot. A lag-time matrix $A(m, n, l)$ corresponds to a path along a torus. We think of n vertical clocks (or wheels) on the torus, each enumerated with symbols $0, \dots, m - 1$. An element a_{ij} of the matrix $A(m, n, l)$ corresponds to the numeral a_{ij} on the j^{th} clock. Under this identification the j^{th} column of $A(m, n, l)$ corresponds to the j^{th} clock and the i^{th} row determines the i^{th} loop around the torus. The torus path of $A(m, n, l)$ then passes through each numeral of each clock $\left\lfloor \frac{l}{\gcd(n, lm)} \right\rfloor$ or $\left\lceil \frac{l}{\gcd(n, lm)} \right\rceil$ many times; in particular if the path is not a torus knot, then it passes through each numeral at least once. (This is Theorem 4.2.) Two loops are equivalent if their corresponding rows are such in $A(m, n, l)$. In this way the equivalence class $\mathbf{eq}(i, j)$ determines an equivalence class of numerals on the j^{th} clock, and so the same number of loops pass through

any two equivalent numerals on the same clock. This common value is either $\left\lfloor \frac{l}{\gcd(n,lm)} \right\rfloor$ or $\left\lceil \frac{l}{\gcd(n,lm)} \right\rceil$. (This is Theorem 5.4.) Define a block β of loops to be $K = l/\gcd(l, r_1)$ inequivalent loops. Then the number of loops passing through a numeral k on the j^{th} clock equals the number of loops in β that pass through numerals equivalent to k . This common value is either $\left\lfloor \frac{l}{\gcd(n,lm)} \right\rfloor$ or $\left\lceil \frac{l}{\gcd(n,lm)} \right\rceil$. (This is Theorem 5.5.) Given $S(m, n, l)$, the foregoing results provide a decomposition of the associated torus path into loops modulo an equivalence relation induced from that on the corresponding lag-time matrix $A(m, n, l)$.

ACKNOWLEDGEMENTS. We are greatly indebted to Hendrik W. Lenstra Jr. for allowing us to include his proof of Theorem 2.3. Moreover we owe a great deal of gratitude to the referee whose comments and suggestions have led to a much clearer and ultimately nicer paper. As well, we very much thank Jim Osterburg and Declan Quinn for their thoughtful comments regarding this paper. Finally we wish to thank Don Passman. This paper honors a great mathematician and teacher. It also honors a wonderful individual and friend.

References

- [FLP] B. Foster, A. Lucas, P. Pappas, “The Subgroup Problem for Lag-Time Sequences,” preprint.
- [La] S. Lang, *Algebra*, Springer-Verlag, New York, 2002.
- [Le] H. W. Lenstra Jr., personal communication, 2004.
- [NST] P. M. Neumann, G. A. Stoy, E. C. Thompson, *Groups and Geometry*, Oxford Science Publications, Oxford University Press, Oxford, 1999.

DEPARTMENT OF MATHEMATICS, BRANDEIS UNIVERSITY, WALTHAM, MA 02454

E-mail address: `rabetz@brandeis.edu`

DEPARTMENT OF BIostatISTICS, JOHNS HOPKINS BLOOMBERG SCHOOL OF PUBLIC HEALTH, BALTIMORE, MD 21205

E-mail address: `seckel@jhsph.edu`

DEPARTMENT OF MATHEMATICS, VASSAR COLLEGE, POUGHKEEPSIE, NY 12604

E-mail address: `pepappas@vassar.edu`

DEPARTMENT OF MATHEMATICS, VASSAR COLLEGE, POUGHKEEPSIE, NY 12604