ACTA ARITHMETICA
LV (1990)

On some Markov matrices arising from the generalized Collatz mapping

by

R. N. Buttsworth and K. R. Matthews (St. Lucia, Qld.)

1. Introduction. In two recent papers [4], [5] the following mapping $T\colon \boldsymbol{Z}\to\boldsymbol{Z}$ has been studied: Let $d\geqslant 2$ be a positive integer and $m_0,\ldots,m_{d-1}$ be non-zero integers. Also R is a complete set of residues mod d and for $i=0,\ldots,d-1$, the residue $r_i\in R$ is defined by $r_i\equiv im_i\ (\mathrm{mod}\ d)$. Then the mapping T is defined by

$$T(x)=\frac{m_i x-r_i}{d}\quad \text{if } x\equiv i\ (\mathrm{mod}\ d). \tag{1.1}$$

The prototype of T was discovered by L. Collatz in 1937 [3] and corresponds to the choice $d=2$, $m_0=1$, $m_1=3$, $R=\{0,-1\}$, i.e.

$$T(x)=\begin{cases} x/2 & \text{if } x \text{ is even},\\ (3x+1)/2 & \text{if } x \text{ is odd}.\end{cases} \tag{1.2}$$

A central property of mapping (1.1) is that the inverse image of a residue class mod m is a union of residue classes mod md. (See [5], Lemma 2.1.) For example if T is the mapping (1.2) and $B(j,m)=\{k\in\boldsymbol{Z}\colon k\equiv j\ (\mathrm{mod}\ m)\}$, we find

$$T^{-1}(B(j,m))=\begin{cases} B(2j,2m)\cup B\left(\frac{2j-1}{3},2m\right) & \text{if } m\not\equiv 0\ (\mathrm{mod}\ 3),\\ B(2j,2m) & \text{if } m\equiv 0\ (\mathrm{mod}\ 3) \text{ and } j\not\equiv 2\ (\mathrm{mod}\ 3),\\ B(2j,2m)\cup B\left(\frac{2j-1}{3},\frac{2m}{3}\right) & \\ \qquad\qquad \text{if } m\equiv 0\ (\mathrm{mod}\ 3) \text{ and } j\equiv 2\ (\mathrm{mod}\ 3).\end{cases} \tag{1.3}$$

Of special interest are the T-invariant subsets of $\boldsymbol{Z}$ (i.e. subsets S of $\boldsymbol{Z}$ satisfying $T(S)\subseteq S$), as the behaviour of the iterates of T can be studied separately on each such set S. We are interested in *T-invariant sets* mod m, i.e. T-invariant sets consisting of residue classes mod m. Those which contain no proper T-invariant set mod m are called *ergodic sets* mod m (previously called minimal

T-invariant sets mod m in [5]). Distinct ergodic sets mod m are disjoint and if $r(m)$ is the number of ergodic sets mod m, then

$$(1.4) \qquad \boldsymbol{Z} = S_0^{(m)} \cup S_1^{(m)} \cup \ldots \cup S_{r(m)}^{(m)},$$

a disjoint union, where $S_1^{(m)}, \ldots, S_{r(m)}^{(m)}$ are the ergodic sets mod m and $S_0^{(m)}$ is the union of the remaining residue classes mod m which we call *transient classes* mod m. In [5] it was conjectured that each divergent trajectory x, $T(x), \ldots, T^{(n)}(x), \ldots$ eventually enters some ergodic set S mod m and that each residue class mod m contained in S is eventually occupied by some iterate, with positive limiting frequency. Also if S is an ergodic set mod d, it was conjectured in [5] that either all trajectories starting in S become trapped in a cycle, or most trajectories starting in S are divergent.

The present paper gives information about the structure of ergodic sets mod m (as m varies).

THEOREM. *Suppose that* $\gcd(m_i, d) = 1$ *for* $0 \leqslant i \leqslant d-1$. *Let*

$$\Delta_{i,l} = r_l(d-m_i) - r_i(d-m_l) \quad \textit{for } 0 \leqslant i < l \leqslant d-1$$

and let

$$\Delta = \Delta(T) = \gcd_{0 \leqslant i < l \leqslant d-1} \Delta_{i,l}.$$

(1) *If m is composed of primes dividing $m_0 \ldots m_{d-1}$, there is only one ergodic set* mod m (*i.e.* $r(m) = 1$); (Example 1.3 shows that this ergodic set may change as m varies. For example take $m = 3$ and 9).

(2) *Assume that* $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$. *Then*

(a) *if* $\gcd(m, \Delta) = 1$, $\boldsymbol{Z}$ *is the only ergodic set* mod m,

(b) *if* $\gcd(m, \Delta) = \delta > 1$, *the ergodic sets* mod m *are just the ergodic sets* mod δ. *In particular, if p is prime, $p^t \| \Delta$, then the ergodic sets* mod p^s *are those* mod p^t, *if* $s \geqslant t$.

The Theorem gives no information if $m = m'm''$, where $\gcd(m', m'') = 1$, m' is composed of primes dividing $m_0 \ldots m_{d-1}$ and $\gcd(m'', \prod_{i=0}^{d-1} m_i) = 1$. However Conjecture 2 below fills this gap. In some cases the Theorem enables us to completely determine all ergodic sets.

EXAMPLE 1.1. If T is the Collatz mapping (1.2) then the ergodic sets mod m are $\boldsymbol{Z}$ if $3 \nmid m$ and $\boldsymbol{Z} \setminus 3\boldsymbol{Z}$ if $3|m$. More generally, if $T_k(x) = x/2$ for even x, $(3x+k)/2$ for odd x, where k is relatively prime to 6, the picture is much more complicated. Let $\delta | k$, $\delta > 1$. Then the ergodic sets $S_i^{(\delta)}(k)$ mod δ are the orbits of the action of the group generated by the permutations $j \to 2j$ and $j \to 3j$ (mod δ) on $\boldsymbol{Z}_m = \boldsymbol{Z}/m\boldsymbol{Z}$. If $3 \nmid m$ and $\gcd(m, k) = 1$, then $\boldsymbol{Z}$ is the only ergodic set mod m. If $3 \nmid m$ and $\gcd(m, k) = \delta > 1$, the ergodic sets mod m are the ergodic sets $S_i^{(\delta)}(k)$ mod δ. If $3|m$ and $\gcd(m, k) = 1$, then $\boldsymbol{Z} \setminus B(0, 3)$ is the only ergodic set mod m. If $3|m$ and $\gcd(m, k) = \delta > 1$, then the ergodic sets mod m are the sets $(\boldsymbol{Z} \setminus B(0, 3)) \cap S_i^{(\delta)}(k)$. For example if $k = 23$, there are 3 ergodic sets mod 23: $B(0, 23)$ and the subsets of $\boldsymbol{Z}$ corresponding to the quadratic residues and quadratic non-residues mod 23, respectively.

If $3^r \| k$, $r \geqslant 1$, there is a related classification of the ergodic sets, with the additional complication that the ergodic sets mod 3^t, $t \geqslant 1$, are now given by $B(0, 3^t)$ if $t \leqslant r$ and $B(0, 3^r) \setminus B(0, 3^{r+1})$ if $t > r$.

EXAMPLE 1.2. If T is the mapping defined by

$$(1.5) \qquad T(x) = \begin{cases} x/2 & \text{if } x \text{ is even,} \\ (5x-3)/2 & \text{if } x \text{ is odd,} \end{cases}$$

then the ergodic sets mod m are $\boldsymbol{Z}$ if $(m, 15) = 1$, $3\boldsymbol{Z}$ and $\boldsymbol{Z} \setminus 3\boldsymbol{Z}$ if $3|m$ and $5 \nmid m$, $\boldsymbol{Z} \setminus 5\boldsymbol{Z}$ if $3 \nmid m$ and $5|m$, $3\boldsymbol{Z} \setminus 5\boldsymbol{Z}$ and $(\boldsymbol{Z} \setminus 3\boldsymbol{Z}) \setminus 5\boldsymbol{Z}$ if $15|m$.

At one stage we believed that there were only finitely many ergodic sets mod m as m varies over all integers. However the following mapping gives a counterexample.

EXAMPLE 1.3. If T is the mapping defined by

$$(1.6) \qquad T(x) = \begin{cases} 3x/2 & \text{if } x \text{ is even,} \\ (3x+1)/2 & \text{if } x \text{ is odd,} \end{cases}$$

then the ergodic sets mod m are $\boldsymbol{Z}$ if $3 \nmid m$ and $T^t(\boldsymbol{Z})$ if $3^t \| m$. The sets $T^t(\boldsymbol{Z})$ consist of 2^t residue classes mod 3^t and are hence distinct as t varies.

Let $m|n$, $m < n$. Then Example 1.3 illustrates the fact that if S is an ergodic set mod m, then S is a T-invariant set mod n, but will not necessarily be an ergodic set mod n. All we can say is that S will be a union of transient classes and one or more ergodic sets mod n. (For example, take $m = 3$, $n = 9$, $S = B(0, 3) \cup B(2, 3)$.) We can show (see Lemma 2.3) that if $B(j, m)$ is a transient class mod m, then the n/m residue classes mod n which comprise $B(j, m)$ are transient classes mod n. Equivalently, if $B(j, n)$ is contained in an ergodic set mod n, then $B(j, m)$ is contained in an ergodic set mod m. Consequently an ergodic set S mod n is contained in exactly one ergodic set mod m if $m|n$. Computer evidence suggests that the following conjectures hold:

CONJECTURE 1. *If* $S = B(j_1, n) \cup \ldots \cup B(j_t, n)$ *is an ergodic set* mod n, *then*

$$\Phi_{n,m}(S) = B(j_1, m) \cup \ldots \cup B(j_t, m)$$

is an ergodic set mod m *if* $m|n$.

CONJECTURE 2. *If S and S' are ergodic sets* mod m *and* m' *respectively, where* $\gcd(m, m') = 1$ *and* $\gcd(m', m_i) = 1$ *for* $i = 0, \ldots, d-1$, *then* $S \cap S'$ *is an ergodic set* mod mm'.

We use standard theory of Markov matrices (see [2], [6]). Using the same notation as in [5], $T^{-1}(B(j, m)) \cap B(k, m)$ is a disjoint union of $p_{jk}(m)$ residue classes mod md. Then (see [5], Lemma 2.9), if $q_{jk}(m) = p_{jk}(m)/d$, $0 \leqslant j, k \leqslant m-1$, the matrix $Q_T(m) = [q_{jk}(m)]$ is an $m \times m$ Markov matrix, i.e. a matrix whose elements are non-negative and whose columns sum to unity. If $d \mid m$, a simple formula exists for $q_{jk}(m)$:

$$q_{jk}(m) = \begin{cases} 1/d & \text{if } j \equiv T(k) \pmod{m/d}, \\ 0 & \text{otherwise}. \end{cases} \tag{1.7}$$

However, if $d \nmid m$, the formula is not so simple. (See [5], Lemma 2.4.) As in [5], a subset S' of $\mathbf{Z}_m = \mathbf{Z}/m\mathbf{Z}$ is *closed with respect to* $Q_T(m)$ if

$$B(k, m) \in S' \text{ and } B(j, m) \notin S' \Rightarrow q_{jk}(m) = 0.$$

Under the 1-1 correspondence (see [5], Lemma 3.1)

$$B(j_1, m) \cup \ldots \cup B(j_t, m) \leftrightarrow \{B(j_1, m), \ldots, B(j_t, m)\}, \tag{1.8}$$

T-invariant sets mod m correspond to closed subsets of $\mathbf{Z}_m$ with respect to $Q_T(m)$, with ergodic sets corresponding to minimal closed sets of $Q_T(m)$. In practice we determine ergodic sets mod m by finding the minimal closed sets of $Q_T(m)$, using a computer implementation of an algorithm in [1].

If S is a T-invariant set mod m, we let $M_m(S)$ denote the submatrix of $Q_T(m)$ formed by the rows and columns which correspond to the residue classes mod m in S. Then S is an ergodic set mod m if and only if $M_m(S)$ is an irreducible matrix. Also if the rows and columns of $Q_T(m)$ are relabelled so that in relation to the partition (1.4), states in $S_i^{(m)}$ precede those in $S_j^{(m)}$ if $i < j$, the matrix $Q_T(m)$ takes on a simpler form:

$$Q_T(m) \sim \begin{bmatrix} D_0(m) & 0 & 0 & \ldots & 0 \\ B_1(m) & M_m(S_1^{(m)}) & 0 & \ldots & 0 \\ B_2(m) & 0 & M_m(S_2^{(m)}) & \ldots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ B_{r(m)}(m) & 0 & 0 & \ldots & M_m(S_{r(m)}^{(m)}) \end{bmatrix} \tag{1.9}$$

where $M_m(S_1^{(m)}), \ldots, M_m(S_{r(m)}^{(m)})$ are irreducible matrices and $(D_0(m))^K \to 0$ as $K \to \infty$. (See [6], p. 296.) One special type of irreducible matrix is a *primitive* (or *regular*) Markov matrix. This is a matrix A for which a suitable power A^K has all its elements positive. For such a matrix we let $i(A)$, the *index of primitivity* of A, be the least such positive integer K. If $m = d^t$, it is implicit in [4], Lemma 5, and Lemma 2.5 below that $i(Q_T(m)) = t$.

2. Some basic properties of transient and ergodic sets mod m. The following result is a consequence of [5], Lemma 3.1.

LEMMA 2.1. *If* $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$, *there are no transient classes* mod m.

The following result is a consequence of [6], Lemma 3.5.27, p. 322:

LEMMA 2.2. $B(j, m)$ *is a transient class* mod m *if and only if* $\sum_{K=0}^{\infty} q_{jj}^{(K)}(m)$ *converges, where*

$$[q_{jk}^{(K)}(m)] = (Q_T(m))^K.$$

Also if $B(j, m)$ *is a transient class* mod m *and* $B(k, m)$ *is an arbitrary residue class* mod m, *then* $\sum_{K=0}^{\infty} q_{jk}^{(K)}(m)$ *converges.*

From Lemma 2.2 we easily deduce the following two results:

LEMMA 2.3. *Let* $B(j, m)$ *be a transient class* mod m. *Then if* $m \mid n$, *the* n/m *residue classes* mod n *which comprise* $B(j, m)$ *are transient classes* mod n.

LEMMA 2.4. *If* $B(j, m)$ *is contained in an ergodic set* S mod m *and* S *does not split into more than one ergodic set* mod n, *where* $m \mid n$, *then not all the component residue classes of* $B(j, m)$ mod n *are transient classes* mod n.

For example, if T is the Collatz mapping, then $B(0, 3)$ is a transient class mod 3, so if $3 \mid m$, residue classes $B(3t, m)$, $t = 0, \ldots, m/3-1$ are transient classes mod m.

Our proofs of primitivity are based on the following property of $Q_T(m)$. (See [5], Lemma 2.8.)

LEMMA 2.5. $T^{-K}(B(j, m)) \cap B(k, m)$ *consists of a disjoint union of* $p_{Kjk}(m)$ *residue classes* mod md^K, *where*

$$(Q_T(m))^K = \left[\frac{p_{Kjk}(m)}{md^K}\right]. \tag{2.1}$$

The next result gives part (1) of the Theorem.

LEMMA 2.6. *If* m *is composed of primes, each dividing* $m_0 \ldots m_{d-1}$, *then there is only one ergodic set* S mod m. *Moreover* $M_m(S)$ *is primitive.*

Proof. If m is a product of k primes (not necessarily distinct) each dividing some m_i, then the proof of [5], Corollary 3.4, generalizes to show that $Q_{T^k}(m)$ has a row of non-zero elements and so has precisely one ergodic set. Then the identity

$$Q_{T^k}(m) = [Q_T(m)]^k \tag{2.2}$$

(which is a restatement of (2.1)) shows that $Q_T(m)$ also has precisely one ergodic set.

Remark 2.1. Lemmas 2.4 and 2.6 show that Conjecture 1 is true if m and n are composed of primes dividing $m_0 \dots m_{d-1}$.

The following definition is standard. (See [2], p. 45.)

If $0 \leqslant j, k \leqslant m-1$, we say $B(j, m)$ is *equivalent* to $B(k, m)$ (with respect to $Q_T(m)$) if there exist $r, s \geqslant 0$, such that $q_{jk}^{(r)}(m) > 0$ and $q_{kj}^{(s)}(m) > 0$, i.e.

$$T^{-r}(B(j, m)) \cap B(k, m) \neq \emptyset \quad \text{and} \quad T^{-s}(B(k, m)) \cap B(j, m) \neq \emptyset. \tag{2.3}$$

This does in fact define an equivalence relation on $\boldsymbol{Z}_m$. A closed set is a union of equivalence classes and the minimal closed sets are precisely the closed equivalence classes.

LEMMA 2.7. *Let* $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$ *and suppose that S is an ergodic set* mod m. *Then for each* $t \geqslant 1$, *S is also an ergodic set* mod md^t. *Moreover, if* $M_m(S)$ *is primitive, so is* $M_{md^t}(S)$ *and* $i(M_{md^t}(S)) \leqslant i(M_m(S)) + t$.

Proof. Suppose that $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$. Assume that S is an ergodic set mod m and that $B(j, m)$ and $B(k, m)$ are contained in S. Then $B(j, m)$ and $B(k, m)$ are equivalent mod m and (2.3) holds for some $r, s \geqslant 0$. We show that (2.3) also holds with m replaced by md^t. As $T^t(k) \in S$, by (2.3) with k replaced by $T^t(k)$, an integer x exists satisfying

$$\begin{aligned} T^r(x) &\equiv j \pmod{m}, \\ x &\equiv T^t(k) \pmod{m}. \end{aligned} \tag{2.4}$$

Using the notation $m_K(k) = m_i$ if $T^K(k) \equiv i \pmod{d}$, we have

$$T^t(k) = \frac{m_0(k) \dots m_{t-1}(k)}{d^t}\left(k - \sum_{i=0}^{t-1} \frac{r_i(k) d^i}{m_0(k) \dots m_i(k)}\right) = \frac{ak+b}{d^t}, \tag{2.5}$$

where a and b are integers, with $\gcd(a, m) = 1$.

Then (2.4) gives

$$x \equiv \frac{ak+b}{d^t} \pmod{m} \tag{2.6}$$

and hence

$$k \equiv \frac{d^t x - b}{a} \pmod{md^t}. \tag{2.7}$$

Let y_0 be an integer satisfying

$$y_0 \equiv \frac{d^t x - b}{a} \pmod{md^{r+t}}. \tag{2.8}$$

Also let

$$y = y_0 + cmd^{r+t}, \tag{2.9}$$

where c is an arbitrary integer. Then

$$T^t(y) = T^t(y_0) + cMmd^r, \tag{2.10}$$

where M is a product of m_i's.

Now from (2.7) and (2.8)

$$y_0 \equiv k \pmod{md^t}, \tag{2.11}$$

so $T^K(y_0) \equiv T^K(k) \pmod{d}$ and hence $m_K(y_0) = m_K(k)$, for $K = 0, \dots, t$. Consequently (2.5) gives

$$T^t(y_0) = \frac{ay_0+b}{d^t}. \tag{2.12}$$

Hence from (2.8)

$$T^t(y_0) \equiv x \pmod{md^r}$$

and (2.10) gives

$$T^t(y) = x + (c_1 + cM) md^r.$$

Hence

$$\begin{aligned} T^{r+t}(y) &= T^r(x) + (c_1 + cM) M' m \\ &= (j + c_2 m) + (c_1 + cM) M' m \\ &= j + m(c_2 + c_1 M' + cMM'), \end{aligned} \tag{2.13}$$

where M' is a product of m_i's.

Since $\gcd(d, MM') = 1$, we may choose c so that $c_2 + c_1 M' + cMM' \equiv 0 \pmod{d^t}$. Then (2.13) gives

$$T^{r+t}(y) \equiv j \pmod{md^t}. \tag{2.14}$$

Also, from (2.9) and (2.11)

$$y \equiv y_0 \equiv k \pmod{md^t}. \tag{2.15}$$

Finally, from (2.14) and (2.15), we have

$$T^{-(r+t)}(B(j, md^t)) \cap B(k, md^t) \neq \emptyset.$$

LEMMA 2.8. *Let* $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$ *and suppose that S is an ergodic set* mod m. *Then if m' is composed of primes dividing d, S is also an ergodic set* mod mm'. *Moreover, if* $M_m(S)$ *is primitive, so is* $M_{mm'}(S)$.

Proof. If m, m' and S are as above, there exists an integer t such that $m'|d^t$. Then $mm'|md^t$ and the fact that S is an ergodic set mod md^t implies that S must also be an ergodic set mod mm'. The primitivity result follows from Lemma 2.5.

3. The proof of the Theorem.

We start with the following easily proved result.

LEMMA 3.1. *If* $\gcd(m, \sum_{i=0}^{d-1} m_i) = 1$, *then*

$$T^{-1}(B(j, m)) = \bigcup_{i=0}^{d-1} B\left(\frac{dj+r_i}{m_i}, md\right) \tag{3.1}$$

is a disjoint union of d residue classes mod md. *More generally, if* $r \geqslant 1$,

$$T^{-r}(B(j, m)) = \bigcup_{i_1=0}^{d-1} \dots \bigcup_{i_r=0}^{d-1} B\left(\frac{d^t}{m_{i_1} \dots m_{i_r}} j + \sum_{l=1}^{r} \frac{d^{l-1} r_{i_l}}{m_{i_1} \dots m_{i_l}}, md^r\right) \tag{3.2}$$

is a disjoint union of d^r residue classes mod md^r.

From (3.2) we deduce

LEMMA 3.2. *If* $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$, *then* $T^{-r}(B(j, m)) \cap B(k, m) \neq \emptyset$ *if and only if there exist* $i_1, \dots, i_r$ *such that*

$$\frac{d^t}{m_{i_1} \dots m_{i_r}} j + \sum_{l=1}^{r} \frac{d^{l-1} r_{i_l}}{m_{i_1} \dots m_{i_l}} \equiv k \pmod{m}. \tag{3.3}$$

(3.3) can be rewritten in terms of affine transformations on $\boldsymbol{Z}_m$. Let $L_m(a, b)$ denote the transformation $j \to aj+b \pmod{m}$, where a and b are rationals with denominators relatively prime to m. Then the following is easily proved by induction.

LEMMA 3.3.

$$L_m(a_r, b_r) \dots L_m(a_1, b_1) = L_m(a, b), \tag{3.4}$$

where

$$a = \prod_{l=1}^{r} a_l \quad \text{and} \quad b = \sum_{l=1}^{r} \left(\prod_{t=1}^{l-1} a_t\right) b_l. \tag{3.5}$$

LEMMA 3.4. *Let a and b be rationals with denominators relatively prime to m. Also suppose that the numerator of a is also relatively prime to m. Then*

$$L_m^{s(a)}(a, b) = L_m(1, 0), \tag{3.6}$$

where

$$s(a) = \operatorname{lcm} s_p(a), \tag{3.7}$$

with p running over the primes dividing m and where if $p^n \| m$

$$s_p(a) = \begin{cases} p^{2n-1} & \text{if } a \equiv 1 \pmod{p}, \\ \operatorname{ord}_{p^n} a & \text{if } a \not\equiv 1 \pmod{p}. \end{cases} \tag{3.8}$$

Proof. We use the identity

$$L_m^r(a, b) = L_m(a^r, b \sum_{l=0}^{r-1} a^l). \tag{3.9}$$

If $a \equiv 1 \pmod{p}$ then $a^{p^{n-1}} \equiv 1 \pmod{p^n}$. Also in this case we have $\sum_{l=0}^{p^{2n-1}-1} a^l \equiv 0 \pmod{p^n}$. However if $a \not\equiv 1 \pmod{p}$, then

$$\begin{aligned} \operatorname{ord}_{p^n} a = r \pmod{p^n} &\Rightarrow a^r - 1 \equiv 0 \pmod{p^n} \\ &\Rightarrow (a-1) \sum_{l=0}^{r-1} a^l \equiv 0 \pmod{p^n} \\ &\Rightarrow \sum_{l=0}^{r-1} a^l \equiv 0 \pmod{p^n}. \end{aligned}$$

Hence if $s = s(a)$ is defined by (3.7) and $p^n \| m$, then

$$a^s \equiv 1 \pmod{p^n} \quad \text{and} \quad \sum_{l=0}^{s-1} a^l \equiv 0 \pmod{p^n}.$$

Hence

$$a^s \equiv 1 \pmod{m} \quad \text{and} \quad \sum_{l=0}^{s-1} a^l \equiv 0 \pmod{m}. \tag{3.10}$$

Then (3.9) gives (3.6), completing the proof of Lemma 3.4.

If $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$, we define

$$L_m(i) = L_m\left(\frac{d}{m_i}, \frac{r_i}{m_i}\right) \quad \text{for } i = 0, \dots, d-1,$$

then from (3.4) and (3.5) we have

$$L_m(i_r) \dots L_m(i_1)(j) \equiv aj+b \pmod{m}, \tag{3.11}$$

where by (3.5) a and b are given by

$$a = \frac{d^t}{m_{i_1} \dots m_{i_r}} \quad \text{and} \quad b = \sum_{l=1}^{r} \frac{d^{l-1} r_{i_l}}{m_{i_1} \dots m_{i_l}}. \tag{3.12}$$

Then using (3.11), Lemma 3.2 gives

LEMMA 3.5. *If* $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$, *then* $T^{-r}(B(j, m)) \cap B(k, m) \neq \emptyset$ *if and only if there exist* $i_1, \ldots, i_r$ *such that*

$$L_m(i_r) \ldots L_m(i_1)(j) \equiv k \pmod{m}. \tag{3.13}$$

Also let $G_m = \langle L_m(0), \ldots, L_m(d-1)\rangle$ *denote the semigroup formed by all products* $L_m(i_r) \ldots L_m(i_1)$. *Then* G_m *is a group and the ergodic sets* mod m *are just the orbits formed by the action of the permutation group* G_m *on* $\mathbf{Z}_m$.

Proof. The group property follows from Lemma 3.4, while (3.13) shows that the equivalence classes with respect to $Q_T(m)$ are just the orbits formed by the action of the permutation group G_m on $\mathbf{Z}_m$.

The next result shows that the second part of the definition of equivalence in (2.3) follows from the first and is a consequence of Lemmas 3.3 and 3.4.

LEMMA 3.6. *Suppose* $\gcd(m, d\prod_{i=0}^{d-1} m_i) = 1$. *If* $T^{-r}(B(j, m)) \cap B(k, m) \neq \emptyset$, *there exists an integer* s *such that*

$$T^{-r(s-1)}(B(k, m)) \cap B(j, m) \neq \emptyset.$$

The next result is fundamental to the proof of our Theorem.

LEMMA 3.7. *If* $\gcd(m, d\prod_{i=0}^{d-1} m_i) = 1$, *then*

$$L_m^{s_l-1}(l)\,L_m^{s_i-1}(i)\,L_m(l)\,L_m(i) = L_m(1, \Delta_{i,l}/m_i m_l), \tag{3.14}$$

where $s_i = s(d/m_i)$ *and* $\Delta_{i,l}$ *is defined by*

$$\Delta_{i,l} = r_l(d-m_i) - r_i(d-m_l). \tag{3.15}$$

Proof. Let $a = d/m_i$, $b = r_i/m_i$, $u = d/m_l$, $v = r_l/m_l$, $s = s_i$ and $t = s_l$. Then the product in (3.14) has the form

$$L_m^{t-1}(u, v)\,L_m^{s-1}(a, b)\,L_m(u, v)\,L_m(a, b) = L_m(\alpha, \beta),$$

where by (3.5) and (3.10) $\alpha = aua^{s-1}u^{t-1} \equiv 1 \pmod{m}$. Also by (3.5) and (3.10) we have

$$\begin{aligned}\beta &= b+va+b\sum_{e=0}^{s-2} a^e au + v\sum_{f=0}^{t-2} u^f aua^{s-1}\\ &\equiv b+va+b(-a^{s-1})au+v(-u^{t-1})aua^{s-1} \pmod{m}\\ &\equiv b+va-bu-v \equiv v(a-1)-b(u-1) = \Delta_{i,l}/m_i m_l.\end{aligned}$$

From Lemma 3.7 we deduce

LEMMA 3.8. *Let* $\gcd(m, d\prod_{i=0}^{d-1} m_i) = 1$. *Then if*

$$\Delta = \gcd_{0 \leqslant i < l \leqslant d-1} \Delta_{i,l}, \tag{3.16}$$

there exist integers $x_{il} \geqslant 0$ *such that*

$$\prod_{0 \leqslant i < l \leqslant d-1} \left(L_m^{s_l-1}(l)\,L_m^{s_i-1}(i)\,L_m(l)\,L_m(i)\right)^{x_{il}} = L_m(1, \Delta). \tag{3.17}$$

Proof. Since $\gcd(m, m_i m_l) = 1$, one has

$$\Delta = \sum y_{il}\Delta_{il} \equiv \sum \frac{y_{il} m_i m_l \Delta_{il}}{m_i m_l} \pmod{m}. \tag{3.18}$$

Now choose $x_{il} = y_{il} m_i m_l + t_{il} m$ with t_{il} large enough so that all $x_{il} \geqslant 0$. Then since $L_m^r(1, b) = L_m(1, rb)$, by (3.14) and (3.18) the left side of (3.17) equals

$$L_m\left(1, \sum_{0 \leqslant i < l \leqslant d-1} \frac{x_{il}\Delta_{il}}{m_i m_l}\right) = L_m(1, \Delta).$$

Remark 3.1. Equation (3.17) expresses $L_m(1, \Delta)$ as a product of $\sum_{0 \leqslant i < l \leqslant d-1} x_{il}(s_i + s_l)$ transformations $L_m(i)$.

LEMMA 3.9. *If* $\gcd(m, \Delta d\prod_{i=0}^{d-1} m_i) = 1$, *then* $\mathbf{Z}$ *is the only ergodic set* mod m. *Moreover* $Q_T(m)$ *is a primitive matrix.*

Proof. Let $B(j, m)$ and $B(k, m)$ be arbitrary residue classes mod m and assume

$$\gcd(m, \Delta d\prod_{i=0}^{d-1} m_i) = 1.$$

Then there exists $t \geqslant 0$ such that $j + t\Delta \equiv k \pmod{m}$. Also

$$L_m^t(1, \Delta)(j) = L_m(1, t\Delta)(j) = j + t\Delta \equiv k \pmod{m}.$$

Hence by Lemma 3.5, $B(j, m)$ and $B(k, m)$ are equivalent mod m. To prove that $Q_T(m)$ is primitive we let t be any integer $0 \leqslant t \leqslant m-1$. Then using (3.9), one has

$$L_m(1, t\Delta) = L_m^t(1, \Delta) \prod_{0 \leqslant i < l \leqslant d-1} \left(L_m^{s_i}(i)\,L_m^{s_l}(l)\right)^{(m-1-t)x_{il}}. \tag{3.19}$$

Now substituting (3.17) for $L_m(1, \Delta)$, we obtain an expression for $L_m(1, t\Delta)$ as a product of

$$\sum t x_{il}(s_i + s_l) + \sum (m-1-t)\,x_{il}(s_i + s_l) = (m-1)\sum x_{il}(s_i + s_l)$$

transformations $L_m(i)$. Hence by Lemma 3.5, since $j+t\Delta \equiv k \pmod{m}$, we have

$$T^{(m-1)\sum x_{il}(s_i+s_l)}(B(j, m)) \cap B(k, m) \neq \emptyset,$$

and hence every element of $(Q_T(m))^{(m-1)\sum x_{il}(s_i+s_l)}$ is positive.

We now prove part 2(a) of the Theorem. If $\gcd(m, \Delta \prod_{i=0}^{d-1} m_i) = 1$ but $\gcd(m, d) \neq 1$, write $m = m_1 m_2$, where m_1 is a product of primes not dividing d and m_2 is a product of primes dividing d. Then by Lemma 3.9, $\boldsymbol{Z}$ is the only ergodic set mod m_1 and hence by Lemma 2.8, $\boldsymbol{Z}$ is the only ergodic set mod $m_1 m_2 = m$ and part 2(a) of the Theorem is now proved.

We now prove part 2(b) of the Theorem.

LEMMA 3.10. *Let* $\gcd(m, d \prod_{i=0}^{d-1} m_i) = 1$ *and* $\gcd(m, \Delta) = \delta > 1$. *If S is an ergodic set* mod δ, *then S is also an ergodic set* mod m. *Moreover if $M_\delta(S)$ is primitive, so is $M_m(S)$.*

Proof. If $\gcd(m, \Delta) = \delta$, then $\delta = xm + y\Delta$ for some $y \geqslant 0$. Then $\delta \equiv y\Delta \pmod{m}$ and $L_m(1, \delta) = L_m^y(1, \Delta) \in G_m$. Hence if $B(j, \delta)$ and $B(k, \delta)$ are equivalent mod δ, we have $L_\delta(a, b)(j) \equiv k \pmod{\delta}$ for some $L_\delta(a, b) \in G_\delta$. Then $L_m(a, b)(j) \equiv k - t\delta \pmod{m}$ for some $t \geqslant 0$. Hence $L_m^t(i, \delta) \times L_m(a, b)(j) \equiv k \pmod{m}$ and $B(j, m)$ and $B(k, m)$ are equivalent mod m.

The conclusion concerning primitivity is derived in the same way as in Lemma 3.9, using (3.19).

If $\gcd(m, \prod_{i=0}^{d-1} m_i) = 1$ and $\gcd(m, \Delta) = \delta$ but $\gcd(m, d) \neq 1$, an argument similar to that preceding Lemma 3.10 shows that the conclusion of Lemma 3.10 still holds. Consequently part 2(b) of the Theorem has now been proved.

Remark 3.2. There exist mappings T and ergodic sets S mod m for which $M_m(S)$ is not primitive. For example if T is the mapping defined by

$$T(x) = \begin{cases} 7x/2 & \text{if } x \text{ is even,} \\ (7x+3)/2 & \text{if } x \text{ is odd,} \end{cases} \tag{3.20}$$

then

$$Q_T(3) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Hence the ergodic sets mod 3 are $S_1^{(3)} = B(0, 3)$ and $S_2^{(3)} = B(1, 3) \cup B(2, 3)$, as $M_3(S_2^{(3)}) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is an irreducible Markov matrix, periodic with period 2.

Remark 3.3. It is an easy exercise to prove that $B(j, m)$ is an ergodic set mod m if and only if

$$r_l \equiv j(m_l - d) \pmod{m} \tag{3.21}$$

for $l = 0, \ldots, d-1$. Also (3.21) implies that m divides all Δ_{il} and hence Δ. Conversely, if m divides Δ and for every prime factor p of m we have $p \nmid (m_l - d)$ for some l, then (3.21) holds for some j and consequently $B(j, m)$ is an ergodic set mod m. Also G_m is commutative if and only if $m \mid \Delta$.

Remark 3.4. It is not difficult to prove that Conjecture 1 holds if m and n are relatively prime to $m_0 \ldots m_{d-1}$. This follows from (2.3), Lemma 3.5, Lemma 3.6 and Lemma 2.8.

4. Examples.

EXAMPLE 4.1. If T is the Collatz mapping $T(x) = x/2$ for even x, $(3x+1)/2$ for odd x, we have $r_0 = 0$, $r_1 = -1$, $m_0 = 1$ and $m_1 = 3$. Then $\Delta_{01} = -1$ and $\Delta = 1$. Hence if $3 \nmid m$, our Theorem implies that $\boldsymbol{Z}$ is the only ergodic set mod m and that $Q_T(m)$ is primitive. If $3 \mid m$, as remarked earlier, the classes $B(3t, m)$ are all transient. Also it is easy to verify that $\boldsymbol{Z} \setminus B(0, 3)$ is T-invariant mod m. It remains to prove that this set is ergodic mod m. The following lemma is easily proved using the last two parts of (1.3).

LEMMA 4.1. *Let T be the Collatz mapping. If $3 \mid m$ and $3 \nmid j$, there exists j', $3 \nmid j'$, such that*

$$T^{-4}(B(j, m)) \supseteq B(j', 2^4 m/3). \tag{4.1}$$

Repeated application of Lemma 4.1 gives

LEMMA 4.2. *If $3^t \| m$, $t \geqslant 1$ and $3 \nmid j$, then there exists j', $3 \nmid j'$, such that*

$$T^{-4t}(B(j, m)) \supseteq B(j', 2^{4t} m/3^t). \tag{4.2}$$

Now suppose $3 \nmid j$, $3 \nmid k$ and that $m = 3^t n$, where $3 \nmid n$. From (4.2) we have

$$\begin{aligned} T^{-(4t+r)}(B(j, m)) \cap B(k, m) &\supseteq T^{-r}(B(j', 2^{4t} n)) \cap B(k, 2^{4t} m) \\ &= T^{-r}(B(j', 2^{4t} n)) \cap B(k, 2^{4t} n) \cap B(k, 3^t). \end{aligned} \tag{4.3}$$

Then by the primitivity of $Q_T(2^{4t} n)$, there exists r such that

$$T^{-r}(B(j', 2^{4t} n)) \cap B(k, 2^{4t} n)$$

is a nonempty union of residue classes mod $2^{4t+r} n$. Hence by the Chinese remainder theorem, as $\gcd(2^{4t} n, 3^t) = 1$,

$$T^{-r}(B(j', 2^{4t} n)) \cap B(k, 2^{4t} n) \cap B(k, 3^t) \neq \emptyset. \tag{4.4}$$

Then (4.3) and (4.4) show that $T^{-(4t+r)}(B(j, m)) \cap B(k, m) \neq \emptyset$.

Hence $M_m(\boldsymbol{Z} \setminus B(0, 3))$ is primitive and consequently $\boldsymbol{Z} \setminus B(0, 3)$ is an ergodic set mod m.

More generally, if T is the mapping $T_k(x) = x/2$ for even x, $(3x+k)/2$ for odd x, where $k > 0$ is relatively prime to 6, we have $r_0 = 0$, $r_1 = -k$, $m_0 = 1$ and $m_1 = 3$. Then $\Delta_{01} = -k$ and $\Delta = k$ and an argument similar to the previous one goes through, with j' in Lemma 4.2 having the additional property that $B(j', n')$ is equivalent to $B(j, n')$ with respect to $Q_T(n')$, for any n' not divisible by 3. The ergodic sets mod δ, where $\delta | k$, $\delta > 1$, are by Lemma 3.5 the orbits of the group of permutations on $\mathbf{Z}_\delta$ generated by the mappings $j \to 2j$ and $j \to \frac{2}{3}j \pmod{\delta}$ acting on $\mathbf{Z}_\delta$.

EXAMPLE 4.2. Here T is the mapping $T(x) = x/2$ for even x, $(5x-3)/2$ for odd x. Then $\Delta = 3$ and by our Theorem, $\mathbf{Z}$ is the only ergodic set mod m and $Q_T(m)$ is primitive, if $\gcd(m, 15) = 1$. If $5 \not| m$ and $3|m$, then $\gcd(m, 3) = 3$ and the ergodic sets mod m are $B(0, 3)$ and $B(1, 3) \cup B(2, 3)$; also by Lemma 3.10, the corresponding matrices are primitive. If $5|m$, the lemma corresponding to Lemma 4.1 is

LEMMA 4.3. *Let T be the above mapping. If $5|m$ and $5 \not| j$, there exists j', $5 \not| j'$, such that*

$$T^{-8}(B(j, m)) \supseteq B(j', 2^8 m/5). \tag{4.5}$$

Moreover, j' can be chosen so that $3|j$ if and only if $3|j'$.

There is also a result analogous to Lemma 4.2. The final result is that if $5|m$ and $3 \not| m$, then $\mathbf{Z} \setminus 5\mathbf{Z}$ is the only ergodic set mod m. If $15|m$, then $(\mathbf{Z} \setminus 5\mathbf{Z}) \cap 3\mathbf{Z} = 3\mathbf{Z} \setminus 5\mathbf{Z}$ and $(\mathbf{Z} \setminus 5\mathbf{Z}) \cap (\mathbf{Z} \setminus 3\mathbf{Z}) = (\mathbf{Z} \setminus 3\mathbf{Z}) \setminus 5\mathbf{Z}$ are the ergodic sets mod m.

EXAMPLE 4.3. Here T is the mapping $T(x) = 3x/2$ for even x, $(3x+1)/2$ for odd x. Then $\Delta = 1$ and $\mathbf{Z}$ is the only ergodic set mod m if $3 \not| m$. Also $M_m(S)$ is primitive. If $3|m$ we need the following result.

LEMMA 4.4. (a) *If $T(j) \equiv T(k) \pmod{3n}$, then $j \equiv k \pmod{2n}$.*

(b) *Also if $t \geqslant 1$ we have*

$$T^t(B(j, 2^t n)) = B(T^t(j), 3^t n). \tag{4.6}$$

Now suppose $m = 3^t n$, where $3 \not| n$. Then $T^t(\mathbf{Z})$ is a T-invariant set mod $3^t n$ by Lemma 3.6. Also Lemma 4.4(a) shows that the residue classes $B(T^t(j), 3^t n)$ are distinct, for $j = 0, \ldots, 2^t n - 1$. It follows that

$$T^{-t}(B(T^t(j), 3^t n)) = B(j, 2^t n). \tag{4.7}$$

Then an argument similar to that following Lemma 4.2, but using (4.7) instead of (4.2) shows that if $r = i(Q_T(m))$, then $M_{3^t n}^{r+t}(T^t(\mathbf{Z}))$ has all its elements positive and $T^t(\mathbf{Z})$ is an ergodic set mod $3^t n$.

In conclusion, the authors would like to record their deep gratitude to Dr. A. M. Watts for his programming assistance and their thanks to the referee for improving the presentation of the paper.

References

[1] B. L. Fox and D. M. Landi, *An algorithm for identifying the ergodic subchains and transient states of a stochastic matrix*, Communications of the ACM, 11 (1968), 619–621.

[2] D. L. Isaacson and R. W. Madsen, *Markov chains: theory and applications*, Wiley, New York 1976.

[3] J. C. Lagarias, *The 3x+1 problem and its generalizations*, Amer. Math. Monthly 92 (1985), 3–23.

[4] K. R. Matthews and A. M. Watts, *A generalization of Hasse's generalization of the Syracuse algorithm*, Acta Arith. 43 (1984), 167–175.

[5] — — *A Markov approach to the generalized Syracuse algorithm*, ibid. 45 (1985), 29–42.

[6] M. Pearl, *Matrix theory and finite mathematics*, McGraw-Hill, New York 1973.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF QUEENSLAND
St. Lucia, Qld., Australia 4067

Received on 8.3.1988
and in revised form on 15.11.1988 (1798)