Collatz-type Problems with Multiple Divisors

by

Keira Gunn

B.Sc., McMaster University, 2007

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

August 2009

Abstract

The Collatz Conjecture hypothesizes that if a sequence of integers beginning with any positive integer t_0 is recursively defined so that $t_{j+1} = \frac{t_j}{2}$ when t_j is even and $t_{j+1} = 3t_j + 1$ when t_j is odd, then there will be some $j \in \mathbb{N}$ such that $t_j = 1$.

I propose a similar family of problems (which I call systems) involving a set of prime divisors $\{p_1, ..., p_k\}$ and a multiplier m, where the sequence is recursively defined so that $t_{j+1} = \frac{t_j}{p_1}$ if t_j is divisible by p_1, $t_{j+1} = \frac{t_j}{p_2}$ if t_j is divisible by p_2 but not p_1, $t_{j+1} = \frac{t_j}{p_3}$ if t_j is divisible by p_3 but not p_1 or p_2 etc., and if t_j is not divisible by any of the primes, then $t_{j+1} = mt_j + 1$.

Assuming the residues of the terms of these sequences behave randomly modulo $p_1 \cdots p_k$, I propose a multiplicative expectation and data to suggest that this is a reasonable model for these systems. If the expectation is less than 1, as in the case of the Collatz problem, then I hypothesize that any sequence will eventually result in some finite cycle.

As well, if my model for these systems is accurate, then I prove that the inclusion of an increasing prime q to a fixed set of prime divisors will result in an effect that gradually diminishes for the multiplicative expectation of the system.

Contents

List of Tables

Acknowledgements

This work would not have been possible without the guidance and support of my supervisor, Dr. Greg Martin. As well, I would like to thank David Steinberg and Heather Hurley for helping me make it this far, and Puck Saunders for inspiration. Finally, I would like to thank Tamaki Kano for her encouragement.

Chapter 1

Introduction

The Collatz problem, also known as the "3x+1" problem, was first posed by Lothar Collatz in 1937 [3]. The problem is defined by its very simple iterative step: if a number is even then divide by two, and if the number is odd then multiply by three then add one (hence the name "3x+1".)

The famous conjecture states that–given any starting number–if this iteration is repeatedly performed to generate a sequence of numbers, then eventually 1 will be contained in that sequence [3]. While the problem itself seems easy enough, extensive research has yielded no proof to this conjecture. However, as of January 18^{th} of 2009 it has been verified that sequences beginning with any of the numbers up to about 20×2^{58} do eventually reach 1 [5].

Probabilistically, one would expect any such sequence to decrease over time. For large numbers, the effect of the "+1" is negligible and so one only needs to investigate the effects of multiplication by 3 or division by 2. The problem is set up in such a way that division by 2 occurs immediately following any muliplication by 3 (the addition of 1 guarantees the resulting number is even) and so–assuming randomness (which will be better explained in the next chapter)–division by 2 again should occur $\frac{1}{2}$ of the time, and division by 2 yet again should occur $\frac{1}{4}$ of the time, etc. For large numbers, this gives a multiplicative expectation of

$$\frac{3}{2 \cdot 2^{\frac{1}{2}} \cdots 2^{\frac{1}{2^k}} \cdots} = \frac{3}{2^{(1+\frac{1}{2}+\frac{1}{4}+\ldots)}} = \frac{3}{2^2} = \frac{3}{4}.$$

This thesis makes no attempt to prove the "3x+1" conjecture, but seeks to look at a family of related problems in the hopes of gaining some insight. Each problem will be referred to as a "system", denoted by $S(m/\{p_1, ..., p_k\})$ (p_i is prime, and m is coprime to p_i for all i in $1, 2, ..., k$), where the iterative step will include an "mx+1" action (the multiplication of m then addition of 1) followed by division by each p_i until the resulting number is no longer divisible by any of the p_i's. Clearly the resulting number after an iteration is coprime to each p_i. For consistency, the starting number in a sequence will be divided by the p_i's as many times as possible before the first iteration is performed.

It is not a necessity that the number 1 is used for addition, the only requirement on the addition number is that it is coprime to each of the prime divisors. However, using 1 guarantees that the addition operation is as negligible as possible.

After some analysis (which is covered in the next chapter) a multiplicative expectation can be found for each system. An expectation of greater than 1

suggests that sequences are gradually increasing, and so there should be many divergent sequences. An expectation of less than 1 suggests that sequences are gradually decreasing and so all sequences should eventually be contained in some finite cycle. The fifth chapter provides empirical evidence supporting these expectations and the idea that the sequences behave randomly (despite the sequences being predetermined by the initial starting point.)

In addition, an interesting but expected result is proven in chapter four. That is, given a system $S(m/\{p_1, ..., p_k\})$, the expection of $S(m/\{p_1, ..., p_k, q\})$ converges to the expectation of $S(m/\{p_1, ..., p_k\})$ as q goes to infinity.

Throughout this thesis, N will be used to denote the product of $p_1 \cdots p_k$. For convenience, the expression "$a \equiv b$" will mean $a \equiv b \pmod{N}$ unless a different modular base is specified. In addition, the term "principle eigenvector" will refer to the eigenvector corresponding to the eigenvalue $\lambda = 1$ for any probability distribution matrix.

Chapter 2

Calculating Expectation

Assuming a random distribution of the residues, the multiplicative expectation for each system is calculated by finding the frequencies at which a sequence should be divisible by each of the divisors, and then using those frequencies in the upcoming expectation formula.

2.1 The Expectation Formula

Given that a randomly selected integer is divisible by a divisor p, there is a $\frac{1}{p^n}$ probability that it is divisible by p^{n+1} for any $n \geq 0$. Another way of expressing this is that, if there is divisibility by p, then the probability of divisibility by p again is $\frac{1}{p}$, and the divisibility by p a third time is $\frac{1}{p^2}$ and etc..

If we let α_i be the expected frequency of divisibility by the divisor p_i for the system $S(m/\{p_1, ..., p_k\})$, then the expectation $E(S)$ is

$$\begin{aligned} E(S) &= m \prod_{i=1}^{k} \left((\tfrac{1}{p_i})(\tfrac{1}{p_i})^{\frac{1}{p_i}} \cdots (\tfrac{1}{p_i})^{\frac{1}{p_i^n}} \cdots \right)^{\alpha_i} \\ &= m \prod_{i=1}^{k} \left((\tfrac{1}{p_i})^{1+\frac{1}{p_i}+\ldots+\frac{1}{p_i^n}+\ldots} \right)^{\alpha_i} = m \prod_{i=1}^{k} \left(\frac{1}{p_i} \right)^{\alpha_i \frac{p_i}{p_i - 1}}. \end{aligned}$$

For the purposes of this thesis, all systems are of the form $S(m/\{2, p_2, ..., p_k\})$ (see chapter 3 for an explanation). Since the multiplier must be coprime to all the divisors, addition by 1 guarantees that divisibility by 2 must occur after an iteration, so $\alpha_1 = 1$ and $\alpha_1 \frac{p_1}{p_1 - 1} = 2$. This simplifies the expectation to

$$E(S) = m \left(\frac{1}{2} \right)^2 \prod_{i=2}^{k} \left(\frac{1}{p_i} \right)^{\alpha_i \frac{p_i}{p_i - 1}} = \frac{m}{4} \prod_{i=2}^{k} \left(\frac{1}{p_i} \right)^{\alpha_i \frac{p_i}{p_i - 1}}. \tag{2.1}$$

From here it is quite simple to calculate the multiplicative expectation once the values of α_2 through α_k are known.

2.2 Frequencies of Divisibility

Each iteration occurs on one of $p - 1$ coprime residues modulo p. Multiplication by m is a bijection from that set of coprime residues to itself. Addition by 1

will then shift exactly one of those initial $p-1$ residues (the residue that is congruent to $-m^{-1}$, precisely) to the value of 0 modulo p, and will thus grant divisibility by p. Because of this, one could naïvely conclude that the value of each α_i is simply $\frac{1}{p_i-1}$. In fact, as has already been established, this holds true for the case $p_1 = 2$. However, for larger primes there are more complicated interractions taking place between the division processes and the likelihood of resulting in any of the residues.

For example, suppose the system is $S(5/\{2,3\})$. This gives $N = 6$ and the residues 1 and 5. If we start with 5 (mod 6) then $mt_0 + 1 \equiv 2$ and so division by 2 results in either 1 or 4 (mod 6) with equal probabilities of $\frac{1}{2}$. If the result is 4 then a second division takes place resulting in either 2 or 5 (mod 6) with equal probabilities of $\frac{1}{4}$. Division of 2 by 2 should again take place, giving the probability of the resulting number being congruent to 1 (mod 6) a value strictly greater than $\frac{1}{2}$. The probability of the resulting number being congruent to 5 (mod 6) is thus less than $\frac{1}{2}$. Specifically, the probabilities are not equal, which refutes the hypothesis made in the previous paragraph.

If an iteration within a system S is defined to include both the "$mx+1$" action and all divisions that take place (until the resulting number is no longer be divisible by any of the primes), then one method of approaching this problem is to construct the probability distribution matrix (which will be denoted by P_S) for the coprime residues modulo N after each iteration. If a is a random representative of the set $\{a, a+N, ..., a+MN\}$ and $P_{S,M,(b,a)}$ is the probability of a being brought to b (mod N) after one iteration, then $P_{S,(b,a)}$ will be the limit of $P_{S,M,(b,a)}$ as M goes to infinity. In the next section, all probabilities discussed will actually be the limit of probabilities of random representives of the set $\{a, a+N, ..., a+MN\}$ as $M \to \infty$.

Once P_S is constructed, the principal eigenvector will give the long-term expectation of the distribution of the residues. From there, the sum of the expectations of the residues that are congruent to $-m^{-1}$ (mod p_i) will give the overall expectation of being divisible by p_i, which is the value of α_i.

2.2.1 The Probability Distribution Matrix

For the system $S(m/\{p_1, ..., p_k\})$, the matrix P_S can be decomposed into $k+1$ transitional matrices $T_0, ..., T_k$. The first matrix is the $\phi(N) \times N$ probability distribution matrix for the set of coprime residues modulo N into the set of all residues modulo N after the "$mx+1$" action ($T_0(b,a)$ is the probability of anything congruent to a being brought to b (mod N) after the "$mx+1$" action). For $a \in \mathbb{Z}_N^*$, a has a probability of 1 of being brought to $ma+1$ in $\mathbb{Z}_N$, so $T_0(ma+1, a) = 1$ and $T_0(b,a) = 0$ for all $b \not\equiv ma+1$.

For the system $S(5/\{2,3\})$, the first transitional matrix would be given by

$$T_0 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix},$$

where T_0 gives the probabilities of the set $\{1,5\}$ being brought into the set $\{1,2,3,4,5,6\}$ (for T_0 above, and T_1 and T_2 below, the order of the indices in T_0 correspond to the order of presentation of the sets).

For $i \in \{1,...,k\}$, the matrix T_i is the probability distribution matrix for the action of division by p_i, so $T_i(b,a)$ is the probability of anything congruent to a being brought to $b \pmod N$ through division by p_i.

Let $I_i = \{a \in \mathbb{Z}_N | a \text{ coprime to } p_1,...,p_{i-1}\}$. If division takes place in the order the primes are listed, then division by p_1 distributes $\mathbb{Z}_N^* = I_1$ to the set I_2, division by p_2 distributes I_2 to I_3, etc.. Each matrix T_i need only consider the probability distribution from I_i to I_{i+1} after division by p_i. (For our example $S(5/\{2,3\})$, we have $I_1 = \{1,2,3,4,5,6\}, I_2 = \{1,3,5\}$, and $I_3 = \{1,5\}$)

If a is coprime to p_i then division by p_i does not take place, so the "division by p_i" action brings a to a with probability 1. This gives $T_i(a,a) = 1$ and $T_i(b,a) = 0$ for all $b \neq a$. In $S(5/\{2,3\})$, this results in columns $[1,0,0]^T, [0,1,0]^T, [0,0,1]^T$ in T_1 corresponding to $1,3,5$ respectively and columns $[1,0]^T, [0,1]^T$ in T_2 corresponding to $1,5$ respectively.

If p_i divides a then there is a $\frac{1}{p_i}$ probability that division by p_i will result in each of $b_{1,s} \equiv \frac{a}{p_i} + s\frac{N}{p_i}$ for $s \in \{1,...,p_i\}$ (the set of all numbers modulo N that are congruent to a when multiplied by p_i). Because $\frac{a}{p_i} \in I_i$ and $\frac{N}{p_i} = R \cdot p_1 \cdots p_{i-1}$ for some integer R, we have that $b_{1,s} \in I_i$ for each s. Since $\frac{N}{p_i}$ is coprime to p_i, the values of $s\frac{N}{p_i}$ run through all residues modulo p_i, thus the values b_{1_s} also run through all residues modulo p_i. One of these values, say $c_1 = b_{1,s}$ for some s is divisible by p_i again. From there, the numbers $b_{2,s} \equiv \frac{c_1}{p_i} + s\frac{N}{p_i}$ for $s \in \{1,...,p_i\}$ will each have a probability of $\frac{1}{p_i^2}$ of occuring and will all be contained in I_i. As well, one of the values, say c_2, will be divisible by p_1.

For $S(5/\{2,3\})$, consider $2 \in I_1$ and division by 2. $b_{1,1} = \frac{2}{2} + (1)\frac{6}{2} = 4$ and $b_{1,2} = \frac{2}{2} + (2)\frac{6}{2} = 1$. So, $c_1 = 4$. Similarly, $b_{2,1} = 5$ and $b_{2,2} = 2$.

Continuing in this manner, there will be some r, s such that $b_{r,s} = a$ (For division of 2 by 2 in $S(5/\{2,3\})$ it is clear that $r = 2$). In fact, r is the order of p_i in the multiplicative group modulo $\frac{N}{M}$ where M is the product of all primes in $\{p_1,...,p_k\}$ that divide a (so $a = sM$ for some s coprime to $\frac{N}{M}$). If d is the order of p_i, then $ap_i^d = sM \cdot p_i^d$ satisfies both $ap_i^d \equiv sM \pmod{\frac{N}{M}}$ and $ap_i^d \equiv 0 \pmod M$, thus $ap_i^d \equiv sM = a \pmod N$ by the Chinese Remainder Theorem. Since, for any $r < d$ we have $ap_i^d \not\equiv sM \pmod{\frac{N}{M}}$, the Chinese Remainder Theorem also gives that $ap_i^d \not\equiv a \pmod N$. By combining this and the fact that each set of $b_{t,s}$'s runs through *all* numbers such that $b_{t,s}p_i^t = a$,

it is evident that $r = d$ is the first level at which the value a recurs (that is, $b_{d,s} = a$ for some s).

The sequence will then repeat itself in such a manner that $b_{(t+r),s} = b_{t,s}$. Thus the probability of resulting in $b_{t,s}$ (for those $b_{t,s}$ that are not divisible by p_i) is equal to

$$\frac{1}{p_i^t} + \frac{1}{p_i^{t+r}} + \frac{1}{p_i^{t+2r}} + ... = \frac{1}{p^t}\left(1 + \frac{1}{p^r} + \frac{1}{p^{2r}} + ...\right) = \frac{p_i^{r-t}}{p_i^r - 1}. \tag{2.2}$$

So, for any $a \in I_i$ and $b \in I_{i+1}$ (we can use I_{i+1} since we are restricted to elements in I_i that are not divisible by p_i), if r is the least positive integer such that $ap_i^r \equiv a$ and t is the least positive integer such that $bp_i^t \equiv a$ then $T_i(b, a) = \frac{p_i^{r-t}}{p_i^r - 1}$ where t is defined, and 0 elsewhere.

Keeping with the $S(5/\{2, 3\})$ example, corresponding to 2 in T_1 we have the column $[\frac{2^{2-1}}{2^2-1}, 0, \frac{2^{2-2}}{2^2-1}]^T = [\frac{2}{3}, 0, \frac{1}{3}]^T$. The rest of the calculations give

$$T_1 = \begin{bmatrix} 1 & \frac{2}{3} & 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & \frac{1}{3} & 0 & \frac{2}{3} & 1 & 0 \end{bmatrix}$$

and

$$T_2 = \begin{bmatrix} 1 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 \end{bmatrix}.$$

The overall probability distribution matrix, P_S is then calculated by the multiplication of all the transitional matrices as follows:

$$P_S = T_k \cdot T_{k-1} \cdots T_1 \cdot T_0. \tag{2.3}$$

For $S(5/\{2, 3\})$ this results in

$$P_S = \begin{bmatrix} 1 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 1 \end{bmatrix} \begin{bmatrix} 1 & \frac{2}{3} & 0 & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & \frac{1}{3} & 0 & \frac{2}{3} & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{2}{3} \\ \frac{1}{2} & \frac{1}{3} \end{bmatrix}.$$

The principal eigenvector for P_S of this system is $[4, 3]^T$, so the long term probability distribution is $[\frac{4}{7}, \frac{3}{7}]$ for the residues $\{1, 5\}$. Of 1 and 5, the only value which is congruent to $-5^{-1} \pmod 3$ is 1, and so the expected probability of divisibility by 3 is $\frac{4}{7}$. Equation (2.1) gives $E(S) = \frac{5}{4}[(\frac{1}{3})^{\frac{3}{3-1}}]^{\frac{4}{7}} \approx 0.48747$. Since the multiplicative expectation is significantly lower than 1, it is expected that this system should quickly decrease, and eventually result in finite cycles.

A list of several other systems and their multiplicative expectations can be found in Table 5.27.

Chapter 3

Uniqueness of the Principal Eigenvector

The final steps in calculating the expectation require that the eigenvector corresponding to $\lambda = 1$ is unique. Obviously, if there are multiple such eigenvectors then there is significant ambiguity in how to evaluate a_2 through a_k and thus $E(S)$.

This section will show that using $p_1 = 2$ ensures that the principal eigenvector is unique. Showing this can be broken into two parts; first: any residue has a positive probability of being brought to any other residue (or itself) after a finite number of iterations and second: if this is the case, then the steady state vector is unique. The first lemma is a slightly stronger version of the latter.

Proposition 3.1. *Let M be a probability distribution matrix with index set I. If for any $i, j \in I$ there is some $r \in \mathbb{N}$ such that $(M^r)_{(i,j)}$ is non-zero, then there is a unique eigenvector corresponding to the eigenvalue $\lambda = 1$, and that eigenvector has positive entries.*

Proof. Let M be a probability distribution matrix as described in the lemma. According to Perron-Frobenius theorem, there is an eigenvector associated with the eigenvalue $\lambda = 1$, and this vector has non-negative entries [4, Chapter 2].

Let $\vec{v}$ be a non-negative eigenvector (whose entries sum to 1) corresponding to $\lambda = 1$; there must be some non-zero value in $\vec{v}$, so suppose $\vec{v}_{(a)} \neq 0$ for some $a \in I$. According to the hypothesis, for any $k \in I$ there is some s (dependent on k) such that $(M^s)_{(k,a)} > 0$.

$\vec{v}$ is an eigenvector for M corresponding to $\lambda = 1$, so $\vec{v}$ is also an eigenvector for M^s corresponding to $\lambda = 1^s = 1$. We have that that $M^s \cdot \vec{v} = \vec{v}$, and thus $(M^s\vec{v})_{(k)} = \vec{v}_{(k)}$. This gives

$$\vec{v}_{(k)} = (M^s\vec{v})_{(k)} = \sum_{i \in I} (M^s)_{(k,i)}\vec{v}_{(i)} = \sum_{i \in I | i \neq a} (M^s)_{(k,i)}\vec{v}_{(i)} + (M^s)_{(k,a)}\vec{v}_{(a)}.$$

Both $\vec{v}$ and M^s have only non-negative entries. This gives

$$\vec{v}_{(k)} \geq 0 + M^s_{(k,a)}\vec{v}_{(a)}.$$

$M^s_{(k,a)}$ and $\vec{v}_{(a)}$ were selected to be positive, so we have

$$\vec{v}_{(k)} > 0.$$

$\vec{v}_{(k)}$ must be positive for any k therefore $\vec{v}$ has no zero entries.

Now that positivity of the vector is established, uniqueness will be proven.

Let $\vec{u}$ be an eigenvector with positive entries as described above. Suppose $\vec{v}$ is a second linearly independent eigenvector corresponding to $\lambda = 1$. So, any linear combination $a\vec{v} + b\vec{u}$ is also an eigenvector corresponding to $\lambda = 1$ for $a, b \in \mathbb{R}$. Let $c = \min\{\frac{\vec{v}_i}{\vec{u}_i} | i \in I\}$. Consider $\vec{w} = \vec{v} - c\vec{u}$. For each $j \in I$ we have

$$\vec{w}_{(j)} = \vec{v}_{(j)} - \min\{\frac{\vec{v}_{(i)}}{\vec{u}_{(i)}} | i \in I\}\vec{u}_{(j)} \geq \vec{v}_{(j)} - \frac{\vec{v}_{(j)}}{\vec{u}_{(j)}}\vec{u}_{(j)} = 0.$$

So $\vec{w}$ is an eigenvector with non-negative entries. Clearly for the i that elicits the minimum of $\frac{\vec{v}_{(i)}}{\vec{u}_{(i)}}$, we have that $\vec{w}_{(i)} = 0$. Since $\vec{u}$ and $\vec{v}$ are linearly independent, $\vec{w} \neq \vec{0}$. The first part of the proof of the lemma verifies that any non-negative eigenvector must be have all positive entries, so $\vec{w}$ cannot exist and thus $\vec{v}$ cannot exist. The eigenvector is unique. □

The second lemma will address the hypothesis in Proposition 3.1 that for any $i, j \in I$, there is an r such that $(M^r)_{(i,j)}$ is positive.

The proof of the following proposition will go back and forth between the systems $S(m/\{2, p_2, ..., p_k\})$ and $S(m/\{2, p_2, ..., p_k, q\})$. To avoid confusion, N will refer to $2p_2 \cdots p_k$. Since $\mathbb{Z}^*_{Nq} \simeq \mathbb{Z}^*_N \times \mathbb{Z}^*_q$, the coprime residues modulo Nq will be written as coordinates in $\mathbb{Z}^*_N \times \mathbb{Z}^*q$ (written as $[a, b]$).

Given P (the probability distribution matrix for $S(m/\{2, p_2, ..., p_k, q\})$) and $a, b \in \mathbb{Z}^*_{Nq}$, if $(P^k)_{(b,a)} > 0$ for some $k \in \mathbb{N}$ then we will write $a \rightsquigarrow b$. Given $\bar{P}$ (the probability distribution matrix for $S(m/\{2, p_2, ..., p_k\})$) and $a, b \in \mathbb{Z}^*_N$, if $(\bar{P}^h)_{(b,a)} > 0$ for some $h \in \mathbb{N}$ then we will write $a \bar{\rightsquigarrow} b$.

Lemma 3.2. *Let M be a probability distribution matrix with index I, and let $a, b, c \in I$. If $a \rightsquigarrow b$ and $b \rightsquigarrow c$ then $a \rightsquigarrow c$.*

Proof. It suffices to show that $(P^{h_1+h_2})_{(c,a)} > 0$.

Since $a \rightsquigarrow b$ and $b \rightsquigarrow c$ we have $(P^{h_1})_{(b,a)} > 0$ and $(P^{h_2})_{(c,b)} > 0$ for some $h_1, h_2 \in \mathbb{N}$. So

$$\begin{aligned}(P^{h_1+h_2})_{(c,a)} = (P^{h_2}P^{h_1})_{(c,a)} &= \sum_{d \in I}(P^{h_2})_{(c,d)}(P^{h_1})_{(d,a)} \\ &\geq \sum_{d=b}(P^{h_2})_{(c,d)}(P^{h_1})_{(d,a)} = (P^{h_2})_{(c,b)}(P^{h_1})_{(b,a)} > 0.\end{aligned}$$ □

Finally, using the notation in Chapter 2, if $P = T_{k+1} \cdots T_0$, then let $P' = T_k \cdots T_0$. So, P' represents the probability distribution in $S(m/\{2, p_2, ..., p_k, q\})$ *without* division by q. In other words, P' is the probability distribution matrix for $q\mathbb{Z}^*_N$ in $S(m/\{2, p_2, ..., p_k\})$, so we have that $\bar{P}_{(a,b)} = \sum_{c \in \mathbb{Z}_q} P'_{([a,c],[b,d])}$ for any $d \in \mathbb{Z}_q$ (this is proven later as Lemma 4.3). Specifically, if $\bar{P}_{(a,b)} > 0$ then for any $d \in \mathbb{Z}_q$ there is some $c \in \mathbb{Z}_q$ with $P'_{([a,c],[b,d])} > 0$.

For the remainder of this chapter, let $T = T_{k+1}$.

Lemma 3.3. *If $\bar{P}_{(x,a)} > 0$ then $P_{([x,y],[a,-m^{-1}])} > 0$ for any $y \in \mathbb{Z}_q^*$.*

Proof. Let $c' \in \mathbb{Z}_q$ be such that $P'_{([x,c'],[a,-m^{-1}])} > 0$

$$\begin{aligned} P_{([x,y],[a,-m^{-1}])} = (TP')_{([x,y],[a,-m^{-1}])} &= \sum_{b\in\mathbb{Z}_N^*}\sum_{c\in\mathbb{Z}_q^*} T_{([x,y],[b,c])}P'_{([b,c],[a,-m^{-1}])} \\ &\geq \sum_{b=x}\sum_{c=c'} T_{([x,y],[b,c])}P'_{([b,c],[a,-m^{-1}])} \\ &= T_{([x,y],[x,c'])}P'_{([b,c'],[x,-m^{-1}])}. \end{aligned}$$

P' includes the "$mx+1$" action but has no division by q, and so for any $y_1, y_2 \in \mathbb{Z}_{Nq}^*$ such that $P'_{([y_1,y_2],[x,-m^{-1}])} > 0$ it must be true that $[y_1, y_2]$ is divisible by q; therefore $c' \equiv 0 \pmod q$. If d is the multiplicative order of q in $\mathbb{Z}_N^*$, then by equation (2.2), for any $[x', y']$ such that $[x'q^d, y'q^d] = [x, c']$ we have that $T_{([x',y'],[x,0])} > 0$. But, $xq^d \equiv x \pmod N$ and $yq^d \equiv 0 \pmod q$ for any $y \in \mathbb{Z}_q^*$, thus $T_{([x,y],[x,c'])} > 0$.

For any $y \in \mathbb{Z}_q^*$,

$$P_{([x,y],[a,-m^{-1}])} > 0.$$

□

Recall an iteration is the "$mx+1$" action, followed with divisions by the primes $2, p_2, ..., p_k$. So, if ψ is an iteration of x, then $\psi(x) = \frac{mx+1}{2^{r_1}p_2^{r_2}\cdots p_k^{r_k}}$ for some non-negative integers $r_1, ..., r_k$ (note that the result of an iteration in $\mathbb{Z}_N^*$ is not necessarily well-defined). However, an iteration that can be applied to one residue may not be applicable to another depending on divisibilities after the "$mx+1$" action. We will say an iteration ψ is *valid* on x if $\psi(x) = \frac{mx+1}{2^{r_1}p_2^{r_2}\cdots p_k^{r_k}}$ where $r_i \geq 1$ when $mx+1$ is divisible by p_i and $r_i = 0$ if $mx+1$ is not divisible by p_i. Also, we will write $\psi(x) \equiv a$ if $a \in \mathbb{Z}_N^*$ and $2^{r_1}p_2^{r_2}\cdots p_k^{r_k}a \equiv x$.

As a result, $P_{(b,a)} > 0$ if and only if there is a valid iteration ψ such that $\psi(a) \equiv b$ and $a \rightsquigarrow b$ if and only if there is a sequence Ψ of valid iterations on a such that $\Psi(a) \equiv b$.

Lemma 3.4. *Let $x, a \in \mathbb{Z}_N^*$, and $b \in \mathbb{Z}_q^*$. Let $\psi_1, ..., \psi_s$ be a sequence of valid iterations on x such that $\psi_s \circ ... \circ \psi_1(x) \equiv a$. If there is $t \in \{1, ..., s\}$ such that $\psi_t \circ ... \circ \psi_1(b) \equiv 0 \pmod q$ then $[a, b] \rightsquigarrow [x, y]$ for any $y \in \mathbb{Z}_q^*$.*

Proof. Let t be the smallest integer such that $\psi_t \circ ... \circ \psi_1(b) \equiv 0 \pmod q$. So, $\psi_{t-1} \circ ... \circ \psi_1$ is a valid sequence of iterations of b in $S(m/\{2, p_1, ..., p_k, q\})$. Let $\Psi = \psi_{t-1} \circ ... \circ \psi_1$. Then $\Psi(b) \equiv -m^{-1} \pmod q$ must be true.

Using Lemma 3.3 along with the fact that $\bar{P}_{(\psi_t\Psi(a),\Psi(a))} > 0$, we have $P_{([\psi_t\Psi(a),z],[\Psi(a),-m^{-1}])} > 0$ for any $z \in \mathbb{Z}_q^*$, in particular $z = -m^{-1}$. Thus, ψ_t can be amended to ψ_t' in $S(m/\{2, p_1, ..., p_k, q\})$ to satisfy $\psi_t' \circ \Psi([a, b]) = [\psi_t \circ ... \circ \psi_1(a), -m^{-1}]$ and be valid in $S(m/\{2, p_2, ..., p_k, q\})$.

$t' = t+1$ is now the smallest such integer with $\psi_{t'} \circ ... \circ \psi_1(b) \equiv 0 \pmod q$. Inductively, the same procedure as above can be applied until $t' = s$. For $t' = s$, choose $z = y$ instead of $z = -m^{-1}$. As constructed, $\psi_t', ..., \psi_s'$ are valid iterations under $S(m/\{2, p_1, ..., p_k, q\})$, and $\psi_s' \circ ... \circ \psi_t'\Psi(a) \equiv \psi_s \circ ... \circ \psi_1(a) = x$. □

For any valid iteration ψ on $[-m^{-1}, b]$, where $\psi([-m^{-1}, b]) = [x, y]$, define 2ψ so that $2\psi([-m^{-1}, b]) = [x, 2y]$.

Lemma 3.5. *2ψ is a valid iteration on $[-m^{-1}, b]$.*

Proof. It is enough to show that $P_{([x,2y],[-m^{-1},b])} > 0$.

$\psi([-m^{-1}, b]) = [x, y]$ implies that $2^{r_1}p_2^{r_2}\cdots p_k^{r_k}y \equiv mb + 1 \pmod q$ and $2^{r_1}p_2^{r_2}\cdots p_k^{r_k}x \equiv m(-m^{-1})+1 \equiv 0 \pmod N$ for some positive integers $r_1, ..., r_k$. If $r_1 > 1$ then let $r_1' = r_1$, otherwise let $r_1' = r_1 + d_2$ where d_2 is the multiplicative order of 2 in $\mathbb{Z}_q^*$. Then $2^{r_1'-1}p_2^{r_2}\cdots p_k^{r_k}x \equiv 0 \equiv m(-m^{-1}) + 1 \pmod N$, and $2^{r_1'-1}p_2^{r_2}\cdots p_k^{r_k}2y = 2^{r_1'}p_2^{r_2}\cdots p_k^{r_k}y \equiv 2^{r_1}p_2^{r_2}\cdots p_k^{r_k}y \equiv mb+1 \pmod q$ and thus $P([x, 2y], [-m^{-1}, b]) > 0$. □

Proposition 3.6. *Given a system $S = S(m/\{2, p_2, ..., p_k\})$, let $N = 2p_2\cdots p_k$ and let P be the probability distribution matrix of S for the coprime residues of N. Then, for any $i, j \in \mathbb{Z}_N^*$, there is an $r \in \mathbb{N}$ such that $(P^r)_{(i,j)}$ is positive.*

Proof. Using the notation above, this proposition is equivalent to showing that for all $a, b \in \mathbb{Z}_N^*$, we have $a \rightsquigarrow b$.

The proof will proceed by induction on the number of prime divisors.

First, let $k = 1$. We have $p_1 = 2$ and $a = b = 1$. $ma + 1 = 2^sL$ for some odd L, so division by 2^s will occur, resulting in $L \equiv 1 \equiv b$. So, $a \rightsquigarrow b$.

Suppose the statement is true for all $S(m/\{2, p_2, ..., p_k\})$, and consider the system $S(m/\{2, p_2, ..., p_k, q\})$. Let $[a, b] \in \mathbb{Z}_N^* \times \mathbb{Z}^*q$. First, it will be shown that $(a, b) \in \mathbb{Z}_N^* \times \mathbb{Z}_q^*$ can be brought to (a, y) for any $y \in \mathbb{Z}_q^*$.

By the inductive hypothesis, $a \overset{-}{\rightsquigarrow} -m^{-1}$ is true. So, there is some sequence of iterations $\psi_1, ..., \psi_{s-1}$ in $S(m/\{2, p_2, ..., p_k\})$ such that $\psi_{s-1}\circ ...\circ\psi_1(a) = -m^{-1}$. Let $\psi_s(x) = \frac{mx+1}{N}$ be the next iteration in the sequence, and so $\psi_s\circ ...\circ\psi_1(a) \equiv x$ for any $x \in \mathbb{Z}_N^*$. In particular, $\psi_s \circ ... \circ \psi_1(a) \equiv a$.

If for some integer $t \leq s$, we have $\psi_t \circ ... \circ \psi_1(b) \equiv 0 \pmod q$, then Lemma 3.4 gives us that $[a, b] \rightsquigarrow [a, y]$ for any $y \in \mathbb{Z}_q^*$ and so the first part of the proof is complete. So, suppose there is no such t. Thus, $\psi_1, ..., \psi_s$ are valid iterations in $S(m/\{2, p_1, ..., p_k, q\})$. If $\Psi = \psi_s \circ ... \circ \psi_1$, then $\Psi(a, b) = (a, y)$ for some fixed $y \in \mathbb{Z}_q^*$.

For any $b \in \mathbb{Z}_q^*$, if $m_1, ..., m_s$ are the multiplicative representations of the division modulo q that occurs in each iteration (note that this is well defined since these values are coprime to q), then we have the following:

$$\begin{aligned} y = \Psi(b) &\equiv m_s(m(...m_2(m(m_1(mb + 1)) + 1)...) + 1) \\ &\equiv m^s\Big(\prod_{i=1}^{s} m_i\Big)b + \sum_{i=1}^{s}\Big(m^{s-i}\prod_{j=i}^{s} m_j\Big) = Ab + B \end{aligned}$$

for some integers A and B where A is coprime to p_{k+1} (since each m_i and m is coprime to p_{k+1}).

To go forth, it is required that $B \not\equiv 0 \pmod q$. If $B \equiv 0 \pmod q$ then ψ_s can be redefined so that $\psi_s(x) = \frac{mx+1}{N}$ and $\psi_s \circ \psi_{s-1} \circ ... \circ \psi_1(a) \equiv -m^{-1}$, and ψ_{s+1} defined so that $\psi_{s+1}(x) = \frac{mx+1}{N}$ and $\psi_{s+1} \circ \psi_s \circ ... \circ \psi_1(a) \equiv a$. If

$\psi_{s+1} \circ ... \circ \psi_1(b) \equiv 0 \pmod q$, then Lemma 3.4 gives us that $[a,b] \rightsquigarrow [a,y]$ for any $y \in \mathbb{Z}_q^*$, as desired. Otherwise, let $\Psi = \psi_{s+1} \circ ... \circ \psi_1$. We now have $y = \Psi(b) \equiv A'b + B'$, where

$$\begin{aligned} B' &= \sum_{i=1}^{s+1} \Big(m^{s+1-i} \prod_{j=i}^{s+1} m_j \Big) = \sum_{i=1}^{s} \Big(m^{s+1-i} \prod_{j=i}^{s+1} m_j \Big) + m_{s+1} \\ &= m_{s+1} \sum_{i=1}^{s} \Big(m^{s+1-i} \prod_{j=i}^{s} m_j \Big) + m_{s+1} = m_{s+1} m \sum_{i=1}^{s} \Big(m^{s-i} \prod_{j=i}^{s} m_j \Big) + m_{s+1} \\ &= m_{s+1} m B + m_{s+1}. \end{aligned}$$

Since $B \equiv 0 \pmod q$, this gives $B' \equiv m_{s+1} \not\equiv 0 \pmod q$, as required. If used, A' and B' will be referred to as A and B respectively.

If $A \not\equiv 1 \pmod q$, then let d be the multiplicative order of A in $\mathbb{Z}_q^*$, otherwise let $d = q$. If there is some $t \in \{1, ..., s\}$ and $r \in \{1, ..., d\}$ such that $\psi_t \circ ... \circ \psi_1 \Psi^r(b) \equiv 0 \pmod q$ then Lemma 3.4 gives that $[a,b] \rightsquigarrow [a,y]$ for any $y \in \mathbb{Z}_q^*$ as desired. Suppose there is no such t and r, so Ψ^d is a valid sequence of iterations on $[a,b]$.

Each application of Ψ gives $\Psi(x) \equiv Ax + B$. If $A \equiv 1 \pmod q$ then

$$\Psi^d(b) \equiv b + dB = b + qB \equiv b \pmod q.$$

For $A \not\equiv 1 \pmod q$ we have

$$\begin{aligned} \Psi^d(b) &= A(...(A(Ab + B) + B)... + B) = A^d b + B \sum_{i=1}^{d-1} A^i \\ &= A^d b + B\Big(\frac{A^d - 1}{A - 1}\Big) \equiv 1b + 0 = b \pmod q. \end{aligned} \tag{3.1}$$

In either case, $\Psi^d(b) \equiv b \pmod q$.

Ψ^{d-1} satisfies that $\Psi\Psi^{d-1}(b) \equiv b \pmod q$; therefore $A\Psi^{d-1}(b) + B \equiv b \pmod q$ and so $\Psi^{d-1}(b) \equiv \frac{b-B}{A} \pmod q$.

Let $\Phi = (2\psi_s) \circ \psi_{s-1} \circ ... \circ \psi_1 \Psi^{d-2}$. By Lemma 3.5, Φ is a valid sequence of iterations on b, and $\Phi(b) = 2\Psi^{d-1}(b) \equiv 2\frac{b-B}{A}$. Now consider $\Psi \circ \Phi$. If for some $t \in \{1, ..., s\}$ we have $\psi_t \circ ... \circ \psi_1 \circ \Phi(b) \equiv 0 \pmod q$ then Lemma 3.4 gives us that $[a,b] \rightsquigarrow [a,y]$ for any $y \in \mathbb{Z}_q^*$ and so the first part of the proof is complete, otherwise $\Psi \circ \Phi$ is a valid sequence of iterations in $S(m/\{2, p_2, ..., p_k, q\})$ and

$$\Psi \circ \Phi(b) = A\Big(2\frac{b - B}{A}\Big) + B = 2b - B. \tag{3.2}$$

So $[a,b] \rightsquigarrow [a, 2b - B]$.

Let $C_b = \{y \in \mathbb{Z}_q^* | [a,b] \rightsquigarrow [a,y]\}$. In the following manipulations of the group C_b, if any sequence of iterations results in 0 modulo q then, as has been shown, this always results in the conclusion that $[a,b] \rightsquigarrow [a,y]$ for any $y \in \mathbb{Z}_q^*$,

or equivalently that $C_b = \mathbb{Z}_q^*$. Suppose that no sequence of iterations results in 0 modulo q.

Equation (3.1) shows that $[a, b] \rightsquigarrow [a, b]$ through the iterations Ψ^d, so $b \in C_b$. Also, $\Phi' = (2\psi_s) \circ \psi_{s-1} \circ ... \circ \psi_1 \Psi^{d-1}$ is a valid sequence of iterations in $S(m/\{2, p_2, ..., p_k, q\})$ and $\Phi'(b) = 2(\Psi^d(b)) = 2b$; therefore $2b \in C_b$ by Lemma 3.2, and similarly we have that $2^r b \in C_b$ for any integer r. Specifically, $2^{d-1}b \in C_b$ where d is the multiplicative order of 2 in $\mathbb{Z}_q^*$.

Equation (3.2) gives that $[a, 2^{d-1}b] \rightsquigarrow [a, 2(2^{d-1}b) - B] = [a, b - B]$, and thus $b - B \in C_b$. There is some $i \in \mathbb{Z}_q^*$ such that $b \equiv Bi \pmod{q}$, and so by repeating this procedure we can conclude that $\{b, b - B, b - (i-1)B\} \subset C_b$. Applying the procedure once more gives divisibility by q and so, along with Lemma 3.4 we have $[a, b] \rightsquigarrow [a, y]$ for any $y \in \mathbb{Z}_q^*$.

Thus, in *all* cases, we have $[a, b] \rightsquigarrow [a, y]$ for any $y \in \mathbb{Z}_q^*$.

Next, consider any $[x, y]$ in $\mathbb{Z}_N^* \times \mathbb{Z}_q^*$. Using the induction hypothesis, there is a sequence of iterations Ψ under $S(m/\{2, p_1, ..., p_k\})$ that brings a to $x \pmod{N}$. If Ψ brings b to $0 \pmod{q}$ at some point then proposition 3.4 can be invoked to show $[a, b] \rightsquigarrow [x, y]$. If at no point Ψ brings b to $0 \pmod{q}$ then Ψ is valid under $S(m/\{2, p_1, ..., p_k, q\})$ and so $[a, b] \rightsquigarrow [x, \Psi(b)]$. Using the results just established $[x, \Psi(b)] \rightsquigarrow [x, y]$ and thus by Lemma 3.2 $[a, b] \rightsquigarrow [x, y]$. □

Propositions 3.1 and 3.6 combine to form:

Theorem 3.7. *Let P be the probability distribution matrix for the coprime residues of $N = 2p_2 \cdots p_k$ in the system $S(m/\{2, p_2, ..., p_k\})$. Then P has a unique positive eigenvecter corresponding to $\lambda = 1$.*

When $p_1 \neq 2$, problems arise from the fact that division is not guaranteed to occur within each iteration. Suppose that $m \not\equiv 1 \pmod{p_i}$ for each $i \in \{1, ..., k\}$, and let d_i be the multiplicative order of m in $\mathbb{Z}_{p_i}^*$. If $\psi(x) = mx + 1$ then

$$\psi^{d_i}(x) = m^d x + \sum_{j=0}^{d-1} m \equiv x + \frac{m^d - 1}{m - 1} \equiv x \pmod{p_i}.$$

This suggests that the ψ operation will cause any $x \in \mathbb{Z}_{p_i}$ to run a cycle of length d_i. There are $\frac{p_i - 1}{d_i}$ cycles of length d_i, and one cycle of length 1 (the number $\frac{-1}{m-1}$ will return to itself after ψ). Since there are more than 2 cycles in total, there are cycles that do not include 0, and any such cycle is smaller than $\mathbb{Z}_{p_i}^*$. A cycle that does not include $0 \pmod{p_i}$ will never encounter divisibility by p_i. In $\mathbb{Z}_{p_1} \times ... \times \mathbb{Z}_{p_k}$ choose $[a_1, ..., a_k]$ so that a_i is in such a cycle for each i and clearly divisibility by *any* of the primes will never occur. $[a_1, ..., a_k]$ will be part of a cycle of length $\text{lcm}(d_1, ..., d_k) < \phi(p_1 \cdots p_k) = |\mathbb{Z}_{p_1 \cdots p_k}^*|$, and therefore not all of $\mathbb{Z}_{p_1 \cdots p_k}^*$. Any number starting in this cycle can never leave the cycle, so there is an eigenvector whose only non-zero components correspond to elements in the cycle.

When $m \equiv 1 \pmod{p_i}$ for some $i \in \{1, ..., k\}$, the proof used for $p_1 = 2$ above falls apart where equation (3.2) becomes

$$\Psi \circ \Phi(b) = A(p_i \frac{b - B}{A}) + B = p_i b - (p_i - 1)B.$$

Using the same methods it can be shown that $p_i b - (p_i - 1)B \in C_b$. If $p_i \equiv 1 \pmod{q}$ then there is no t such that $b \equiv t(p_i - 1)B \pmod{q}$, and so the proof cannot be continued as before. However, if $p_i \not\equiv 1 \pmod{q}$ then there is such a t and the proof can be concluded similarly to when $p_i = 2$. This results in the following generalization:

Theorem 3.8. *Let $p_1, ..., p_k$ be primes, and $m \equiv 1 \pmod{p_i}$ for some $i \in \{1, ..., k\}$. Let P be the probability distribution matrix for the coprime residues of $N = p_1 \cdots p_k$ in the system $S(m/\{p_1, ..., p_k\})$. If $p_i \not\equiv 1 \pmod{p_j}$ for all $j \in \{1, ..., k\}$ then P has a unique positive eigenvecter corresponding to $\lambda = 1$.*

Chapter 4

The Effect of Increasing a Divisor on Expectation

A brief investigation of Table 5.27 (Multiplicative Expectations for Systems), suggests that as more divisors are added the expectation tends to decrease but if a divisor is increased then the expectation tends to increase as well. Specifically, looking at the systems $S(11/\{2,3,q\})$ (the right-hand side of the table), it appears that as q increases the expectation is generally increasing, but does not appear to surpass the expectation of $S(11/\{2,3\})$. This observation leads to a prediction that the expectation $E(S(m/\{2,p_1,...,p_k,q\})$ should converge to $E(S(m/\{2,p_1,...,p_k\}))$ as $q \to \infty$. In fact, this is Theorem 4.16.

The key to the proof of this theorem is to show that the probability of division by q tends to 0 as q tends to infinity, and thus has minimal effect on the residues modulo N after an iteration (in this case, $N = 2p_2 \cdots p_k$). The proof will proceed by comparing the principal eigenvector of the probability distribution matrix $P(S)$ to that of a similar, but easily controlled matrix P'.

Let $\bar{i}$ be the notation for the residue representative of i in $\mathbb{Z}_N$. Also, let $\bar{P}$ be the probability distribution matrix for $\mathbb{Z}_N^*$ into itself within the system $S(m/\{2,p_2,...,p_k\})$ and let P be the probability distribution matrix for the residue set $S_0 = \{x \in \mathbb{Z}_{Nq} | x \text{ is coprime to } N\}$ into itself within the system $S(m/\{2,p_1,...,p_k,q\})$. If $Q = q\mathbb{Z}_N^*$, then note that $S_0 = \mathbb{Z}_{Nq}^* \cup Q$.

Although the principal eigenvector for $P(S)$ (the probability distribution matrix for $\mathbb{Z}_{Nq}^*$ in S) is ultimately what we are trying to analyse, the next lemma will allow us to substitute this eigenvector for that of P.

Lemma 4.1. *If $\vec{w} \in \mathbb{R}^{\phi(Nq)}$ is the principal eigenvector for $P(S)$ and $\vec{u} \in \mathbb{R}^{\phi(N)q}$ is the principal eigenvector for P, then $\vec{w}_{(a)} = \vec{u}_{(a)}$ for $a \in \mathbb{Z}_{Nq}^*$ and $\vec{u}_{(a)} = 0$ for $a \in Q$.*

Proof. Division by q ensures that after an iteration, no resulting number can be divisible by q. This gives $P_{(a,b)} = 0$ for any $b \in S_0$ when $a \in Q$. So, since $\vec{u}$ is a principal eigenvector for P we have

$$\vec{u}_{(a)} = (P\vec{u})_{(a)} = \sum_{b \in S_0} P_{(a,b)}\vec{u}_{(b)} = \sum_{b \in S_0} (0)\vec{u}_{(b)} = 0.$$

If $a, b \in \mathbb{Z}^*_{Nq}$, then $P(S)_{(a,b)} = P_{(a,b)}$. So, for $a \notin Q$, we then have

$$\vec{u}_{(a)} = (P\vec{u})_{(a)} = \sum_{b\in S_0} P_{(a,b)}\vec{u}_{(b)} = \sum_{b\in Q} P_{(a,b)}\vec{u}_{(b)} + \sum_{b\in\mathbb{Z}^*_{Nq}} P_{(a,b)}\vec{u}_{(b)}$$
$$= \sum_{b\in Q} P_{(a,b)}(0) + \sum_{b\in\mathbb{Z}^*_{Nq}} P(S)_{(a,b)}\vec{u}_{(b)} = \sum_{b\in\mathbb{Z}^*_{Nq}} P(S)_{(a,b)}\vec{u}_{(b)} = \big(P(S)\vec{u}\big)_{(a)}.$$

The only vector in $\mathbb{R}^{\phi(Nq)}$ that satisfies $\vec{u}_{(a)} = \big(P(S)\vec{u}\big)_{(a)}$ for all $a \in \mathbb{Z}^*_{Nq}$ is $\vec{w}$. Thus, we have $\vec{u} = \vec{w}$. □

Using equation (2.3) we can write P as $P = T_{k+1}\cdots T_0$ for the transitional matrices $T_0, ..., T_{k+1}$. For convenience, let $T = T_{k+1}$. Also, let $P' = T_k \cdots T_0$. Specifically, P' is the probability distribution matrix for S_0 into itself within the system $S(m/\{2, p_1, ..., p_k\})$ (notice the omission of division by q). Also, $P = TP'$.

Finally, let $A = \{a \in \mathbb{Z}^*_{Nq} | ma + 1 \equiv 0 \pmod q\} \subset \mathbb{Z}^*_{Nq}$, so A is a subset of S_0.

Lemma 4.2.

$$|A| = |Q| = \phi(N).$$

Proof. $Q = q\mathbb{Z}^*_N$, so $|Q| = |\mathbb{Z}^*_N| = \phi(N)$ is trivial.

$A = \{a \in \mathbb{Z}^*_{Nq} | ma + 1 \equiv 0 \pmod q\}$. By the Chinese Remainder Theorem, in $\mathbb{Z}^*_{Nq}$ there is a unique solution to $a \equiv 0 \pmod q$ and $a \equiv b \pmod N$ for each $b \in \mathbb{Z}^*_N$, thus there are $|\mathbb{Z}^*_N| = \phi(N)$ solutions, and so $|A| = \phi(N)$. □

The first part of the proof of the theorem will be to find a principal eigenvector for the matrix P'. Before we begin, two more lemmas will be useful:

Lemma 4.3. *For any $a, b \in S_0$,*

$$\sum_{c\in S_0 | c\equiv b} P'_{(c,a)} = \bar{P}_{(\bar{b},\bar{a})}.$$

Proof. Recall from earlier that $P' = T_k \cdots T_0$. Similar to Chapter 2, let $I_0 = S_0$ and $I_i = \{a \in \mathbb{Z}_{Nq} | a \text{ coprime to } p_1, ..., p_{i-1}\}$ for $i \in \{1, ..., k\}$. For any $a \in I_i$ and $b \in I_{i+1}$ let $\overline{T_{i(b,a)}} = \sum_{c\in I_{i+1}|c\equiv b} T_{i(c,a)}$. First, it will be shown that $\overline{T_{i(b,a)}} = \bar{T}_{i(\bar{b},\bar{a})}$ for all $i \in \{0, ..., k\}$.

For $i = 0$, the result is simple. $T_{0(ma+1,a)} = 1$ and $T_{0(c,a)} = 0$ for all $c \not\equiv ma + 1 \pmod{Nq}$.

If $b \not\equiv ma + 1 \pmod N$ then $c \not\equiv ma + 1 \pmod{Nq}$ for any $c \equiv b$. Also, $b \not\equiv m\bar{a} + 1 \pmod N$, so $\bar{T}_{0(\bar{b},\bar{a})} = 0$. We have

$$\overline{T_{0(b,a)}} = \sum_{c\in I_{i+1}|c\equiv b} T_{0(c,a)} = \sum_{c\in I_{i+1}|c\equiv b} 0 = 0 = \bar{T}_{0(\bar{b},\bar{a})}.$$

If $b \equiv ma+1 \pmod N$ then $b' \equiv ma+1 \pmod{Nq}$ for a unique $b' \in S_0$ such that $b' \equiv b$. Also, $b \equiv m\bar{a}+1 \pmod N$, so $\bar{T}_{0(\bar{b},\bar{a})} = 1$. We have

$$\begin{aligned}\overline{T_{0(b,a)}} &= \sum_{c\in I_{i+1}|c\equiv b} T_{0(c,a)} = T_{0(b',a)} + \sum_{c\in I_{i+1}|c\equiv b, c\neq b'} T_{0(c,a)} \\ &= 1 + \sum_{c\in I_{i+1}|c\equiv b} 0 = 1 = \bar{T}_{0(\bar{b},\bar{a})}.\end{aligned}$$

When $i \neq 1$, the result is more involved.

For $a \in I_i$ and $b \in I_{i+1}$ suppose $\bar{T}_{i(\bar{b},\bar{a})} = 0$. So, $bp_i^s \not\equiv a \pmod N$ for any $s \in \mathbb{Z}$. Thus, for any $c \equiv b$ we have that $cp_i^s \not\equiv a \pmod{Nq}$ for any $s \in \mathbb{Z}$ and so $\overline{T_{i(b,a)}} = 0$.

Suppose then, that $\bar{T}_{i(\bar{b},\bar{a})} \neq 0$. According to equation (2.2) we have $\bar{T}_{i(\bar{b},\bar{a})} = \frac{p_i^{r-t}}{p_i^r-1}$ where r is the least positive integer such that $ap_i^r \equiv a$ and t is the least positive integer such that $bp_i^t \equiv a$. Suppose that s is the least positive integer such that $ap_i^s \equiv a \pmod{Nq}$. There is some $K \in \mathbb{Z}^+$ such that $s = Kr$. For each $j \in \{0, ..., K-1\}$, the Chinese Remainder Theorem gives a unique solution for $c_j \in I_{i+1}$ with $c_j \equiv b$ such that $c_j p_i^{jr+t} \equiv a \pmod{Nq}$ (and no solution for $c_j p_i^n \equiv a \pmod{Nq}$ where n cannot be written as $n = jr+t$ for some j). Equation (2.2) then gives $T_{i(c_j,a)} = \frac{p_i^{Kr-(jr+t)}}{p_i^{Kr}-1}$ and $T_{i(c,a)} = 0$ for all $c \notin \{c_0, ..., c_{K-1}\}$. We have

$$\begin{aligned}\overline{T_{i(b,a)}} &= \sum_{c\in I_{i+1}|c\equiv b} T_{i(c,a)} = \sum_{j=0}^{K-1} T_{i(c_j,a)} = \sum_{j=0}^{K-1} \frac{p_i^{Kr-(jr+t)}}{p_i^{Kr}-1} = \sum_{j=1}^{K} \frac{p_i^{jr-t}}{p_i^{Kr}-1} \\ &= \frac{p_i^{-t}}{p_i^{Kr}-1} p_i^r \sum_{j=0}^{K-1} p_i^{jr} = \frac{p_i^{-t}}{p_i^{Kr}-1} p_i^r \left(\frac{p_i^{Kr}-1}{p_i^r-1}\right) = \frac{p_i^{r-t}}{p_i^r-1} = \bar{T}_{i(\bar{b},\bar{a})}.\end{aligned}$$

This concludes the first part of the proof of the lemma, that $\overline{T_{i(b,a)}} = \bar{T}_{i(\bar{b},\bar{a})}$ for all $i \in \{0, ..., k\}$. It remains to show that multiplication of these matrices maintains this summation property (with appropriate index sets). That is, that $\overline{P'_{(b,a)}} = \bar{P'}_{(\bar{b},\bar{a})}$ for all $a, b \in S_0$.

Assume the property is held for $T_{j-1} \cdots T_0$, then for any $a \in S_0$ and $b \in I_{j+1}$ we have

$$\begin{aligned}\overline{(T_j \cdots T_0)_{(b,a)}} &= \sum_{c\in I_{i+1}|c\equiv b} (T_j \cdots T_0)_{(c,a)} \\ &= \sum_{c\in I_{i+1}|c\equiv b} \Big(\sum_{d\in I_i} T_{j(c,d)} (T_{j-1} \cdots T_0)_{(d,a)} \Big) \\ &= \sum_{d\in I_i} \Big((T_{j-1} \cdots T_0)_{(d,a)} \sum_{c\in I_{i+1}|c\equiv b} T_{j(c,d)} \Big) \\ &= \sum_{d\in I_i} (T_{j-1} \cdots T_0)_{(d,a)} \overline{T_{j(b,d)}}.\end{aligned}$$

From the previous result, we have that $\overline{T_{j(b,d)}} = \bar{T}_{j(\bar{b},\bar{d})}$. So,

$$\begin{aligned}\overline{(T_j \cdots T_0)_{(b,a)}} &= \sum_{d \in I_i} (T_{j-1} \cdots T_0)_{(d,a)} \bar{T}_{j(\bar{b},\bar{d})} \\ &= \sum_{c \in I_i \cap \mathbb{Z}_N} \sum_{d \in S_0 | d \equiv c} (T_{j-1} \cdots T_0)_{(d,a)} \bar{T}_{j(\bar{b},\bar{d})} \\ &= \sum_{c \in I_i \cap \mathbb{Z}_N} \bar{T}_{j(\bar{b},c)} \sum_{d \in S_0 | d \equiv c} (T_{j-1} \cdots T_0)_{(d,a)} \\ &= \sum_{c \in I_i \cap \mathbb{Z}_N} \bar{T}_{j(\bar{b},c)} \overline{(T_{j-1} \cdots T_0)_{(d,a)}}.\end{aligned}$$

The induction hypothesis now gives

$$\overline{(T_j \cdots T_0)_{(b,a)}} = \sum_{c \in I_i \cap \mathbb{Z}_N} \bar{T}_{j(\bar{b},c)} (\bar{T}_{j-1} \cdots \bar{T}_0)_{(c,\bar{a})} = (\bar{T}_{j+1} \cdots \bar{T}_0)_{(\bar{b},\bar{a})}.$$

$\sum_{c \in S_0 | c \equiv b} P'_{(c,a)} = \bar{P'}_{(\bar{b},\bar{a})}$ follows from the conclusion of the induction argument. □

Lemma 4.4. *For any $a, c \in S_0$,*

$$\sum_{b \in S_0 | b \equiv a} P'_{(c,b)} = \bar{P}_{(\bar{c},\bar{a})}.$$

Proof. As per Section 2.2.1, if $a \in A$, then $P'_{(b,a)} = 0$ for any $b \notin Q$. Using Lemma 4.3 we have

$$\begin{aligned}\bar{P}_{(\bar{c},\bar{a})} &= \sum_{b \in S_0 | b \equiv c} P'_{(b,a)} = \sum_{b \in Q | b \equiv c} P'_{(b,a)} + \sum_{b \notin Q | b \equiv c} P'_{(b,a)} \\ &= \sum_{b \in Q | b \equiv c} P'_{(b,a)} + \sum_{b \notin Q | b \equiv c} (0) = \sum_{b \in Q | b \equiv c} P'_{(b,a)}.\end{aligned}$$

According to the Chinese Remainder Theorem, there is a unique $b \in S_0$ such that $b \equiv 0 \pmod{q}$ and $b \equiv c$, therefore $P'_{(c,a)} = \bar{P}_{(\bar{c},\bar{a})}$ when $c \in Q$ and $a \in A$.

Consider any $c \in Q$. Section 2.2.1 also tells us that if $b \notin A$ then $P'(c, b) = 0$. This combined with the previous result gives

$$\begin{aligned}\sum_{b \in S_0 | b \equiv a} P'_{(c,b)} &= \sum_{b \in A | b \equiv a} P'_{(c,b)} + \sum_{b \notin A | b \equiv a} P'_{(c,b)} \\ &= \sum_{b \in A | b \equiv a} P'_{(c,b)} + \sum_{b \notin A | b \equiv a} 0 = \sum_{b \in A | b \equiv a} P'_{(c,b)}\end{aligned}$$

Again, there is a unique b so that $b \in A$ and $b \equiv a$, so we get

$$\sum_{b \in S_0 | b \equiv a} P'_{(c,b)} = \bar{P}_{(\bar{c},\bar{a})}.$$

Consider $c \notin Q$, so $c \in \mathbb{Z}^*_{Nq}$. For any $b \in S_0$ there is a unique $K \in \mathbb{Z}_{Nq}$ such that $Kc \equiv b \pmod{Nq}$. Suppose $c' \equiv c$, and let K be such that $Kc' \equiv ma + 1 \pmod{Nq}$; there are two cases. Case 1: $K \equiv 2^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ for some sets of integers $\{r_1, ..., r_k\}$ with $0 \leq r_i \leq d_i$ (d_i is the multiplicative order of p_i in $\mathbb{Z}^*_{Nq}$) and Case 2: there are no such $r_1, ..., r_k$.

For Case 2, the operations of $S(m/\{2, p_2, ..., p_k\})$ cannot bring a to c' and therefore $P'_{(c',a)} = 0$. For Case 1, a can be brought to c' and the value of $P'(c', a)$ is determined only by the sets $\{r_1, ..., r_k\}$. In both cases, $P'(c', a)$ depends only on K.

Since $c' \equiv c$, we have $c \equiv c' + dN \pmod{Nq}$ for some integer d. Let $a' \equiv a + KdNm^{-1} \pmod{Nq}$. Then

$$\begin{aligned} ma' + 1 &\equiv m(a + KdNm^{-1}) + 1 \equiv ma + KdN + 1 \equiv Kc' + KdN \\ &\equiv K(c' + dN) \equiv Kc \pmod{Nq}. \end{aligned}$$

Thus there is some a' with $P'(c, a') = P'(c', a)$.

This gives a bijection between the values of $P'(c', a)$ and $P'(c, a')$ for $c' \equiv c$ and $a' \equiv a$. This, along with Lemma 4.3 gives

$$\sum_{b \in S_0 | b \equiv a} P'_{(c,b)} = \sum_{b \in S_0 | b \equiv c} P'_{(b,a)} = \bar{P}_{(\bar{a}, \bar{c})}. \qquad \square$$

Define the vector $\vec{u'}$ by $\vec{u'}_{(a)} = \frac{\vec{v}_{(\bar{a})}}{q}$. Then we have the following proposition, which will be the first step in the proof of the theorem mentioned at the beginning of this chapter:

Proposition 4.5. *$\vec{u'}$ is a principal eigenvector for P'.*

Proof. Consider $w = P'\vec{u'}$. For each $b \in S_0$ we have

$$\begin{aligned} (P'\vec{u'})_{(b)} &= \sum_{a \in S_0} P'_{(b,a)} \vec{u'}_{(a)} = \sum_{c \in \mathbb{Z}^*_N} \sum_{a \in S_0 | a \equiv c} P'_{(b,a)} \vec{u'}_{(a)} \\ &= \sum_{c \in \mathbb{Z}^*_N} \sum_{a \in S_0 | a \equiv c} P'_{(b,a)} \frac{\vec{v}_{(\bar{a})}}{q} = \sum_{c \in \mathbb{Z}^*_N} \sum_{a \in S_0 | a \equiv c} P'_{(b,a)} \frac{\vec{v}_{(c)}}{q} \\ &= \frac{1}{q} \sum_{c \in \mathbb{Z}^*_N} \Big(\vec{v}_{(c)} \sum_{a \in S_0 | a \equiv c} P'_{(b,a)} \Big). \end{aligned}$$

Lemma 4.4 gives

$$(P'\vec{u'})_{(b)} = \frac{1}{q} \sum_{c \in \mathbb{Z}^*_N} \vec{v}_{(c)} \bar{P}_{(\bar{b}, \bar{c})} = \frac{1}{q} \sum_{c \in \mathbb{Z}^*_N} \vec{v}_{(c)} \bar{P}_{(\bar{b}, c)} = \frac{1}{q} (\bar{P}\vec{v})_{(\bar{b})}.$$

Since $\vec{v}$ is the principal eigenvector for $\bar{P}$, this simplifies to

$$(P'\vec{u'})_{(b)} = \frac{1}{q} \vec{v}_{(\bar{b})} = \vec{u'}_{(b)}.$$

For all $b \in S_0$ we have $(P'\vec{u'})_{(b)} = \vec{u'}_{(b)}$, so $\vec{u'}$ is a principal eigenvector for P'. □

The next step of the proof of the theorem is to show that for any $a \in \mathbb{Z}_N^*$, the sum of the values of $\vec{u}_{(b)}$ where $b \equiv a$ converges to $\vec{v}_{(a)}$ as q increases. This will be a result of the similarity between P and P', and thus their eigenvectors.

Several new notations and lemmas will prove useful for the upcoming proposition.

For any real vector $\vec{w}$, we will define the function D on $\vec{w}$ so that $D(\vec{w}) = \sum_{i \in I} |\vec{w}_{(i)}|$, where I is the index set of $\vec{w}$.

Lemma 4.6. *For any real vectors $\vec{u}, \vec{w}$ with index set I and $K \in \mathbb{R}$, the following are true:*
i. $D(K\vec{w}) = K \cdot D(\vec{w})$;
ii. $D(\vec{u}) - D(\vec{w}) \leq D(\vec{u} + \vec{w}) \leq D(\vec{u}) + D(\vec{w})$;
iii. If P is a non-negative matrix with index set I whose columns sum to 1, then $D(P\vec{w}) \leq D(\vec{w})$.

Proof. i. is trivial, and *ii.* is a straightforward result of the triangle inequality. The proof of *iii.* is as follows:

$$D(P\vec{w}) = \sum_{i \in I} |(P\vec{w})_{(i)}| = \sum_{i \in I} \left| \sum_{j \in I} P_{(i,j)} \vec{w}_j \right| \leq \sum_{i \in I} \sum_{j \in I} |P_{(i,j)} \vec{w}_{(j)}|$$
$$= \sum_{i \in I} \sum_{j \in I} P_{(i,j)} |\vec{w}_{(j)}| = \sum_{j \in I} |\vec{w}_{(j)}| \sum_{i \in I} P_{(i,j)} = \sum_{j \in I} |\vec{w}_{(j)}|(1) = D(\vec{w}). \square$$

For P and P' as defined earlier, let $\Delta = P' - P$. So

$$\Delta = P - P' = TP' - P' = (T - I)P'$$

$(T - I)$ will have the form of $\vec{0}$ for all columns with $a \notin Q$. For $a, b \in Q$ and $a \neq b$, we have $(T - I)_{(a,a)} = -1$ and $(T_q - I)_{(a,b)} = 0$. For $a \in Q$ and $b \notin Q$ the values of $(T - I)$ follow the probability distributions described in Section 2.2.1: if there is no integer r such that $bq^r \equiv a \pmod{N}$ then $(T - I)_{(b,a)} = 0$; if there is such an r, and d is the multiplicative order of q in $\mathbb{Z}_N^*$ then by equation (2.2), we have $(T - I)_{(b,a)} = \frac{q^{d-r}}{q^d - 1}$, where $r \in \{1, ..., d\}$. The sum of each column is 0.

Lemma 4.7. *If $\vec{w}$ is a real vector with index set $\mathbb{Z}_{Nq}^*$ then $\sum_{a \in S_0} (\Delta\vec{w})_{(a)} = 0$.*

Proof.

$$\sum_{a \in S_0} (\Delta\vec{w})_{(a)} = \sum_{a \in S_0} \sum_{b \in S_0} \Delta_{(a,b)} \vec{w}_{(b)} = \sum_{b \in S_0} \vec{w}_{(b)} \sum_{a \in S_0} \Delta_{(a,b)}$$
$$= \sum_{b \in S_0} \vec{w}_{(b)}(0) = 0. \qquad \square$$

Lemma 4.8. *If $\vec{u'}$ is the principal eigenvector for P', then $D(\Delta\vec{u'}) = \frac{2}{q}$.*

Proof.

$$\begin{aligned} D(\Delta\vec{u'}) &= D((T-I)P'\vec{u'}) = D((T-I)\vec{u'}) \\ &= \sum_{a\in S_0} |((T-I)\vec{u'})_{(a)}| = \sum_{a\in S_0} \Big| \sum_{b\in S_0} (T-I)_{(a,b)}\vec{u'}_{(b)} \Big| \\ &= \sum_{a\in S_0} \Big| \sum_{b\in Q} (T-I)_{(a,b)}\vec{u'}_{(b)} + \sum_{b\notin Q} (T-I)_{(a,b)}\vec{u'}_b \Big|. \end{aligned}$$

From the construction of $(T-I)$, we have $(T-I)_{(a,b)} = 0$ for $b \notin Q$, so

$$\begin{aligned} D(\Delta\vec{u'}) &= \sum_{a\in S_0} \Big| \sum_{b\in Q} (T-I)_{(a,b)}\vec{u'}_{(b)} + \sum_{b\notin Q} (0)\vec{u'}_b \Big| \\ &= \sum_{a\in Q} \Big| \sum_{b\in Q} (T-I)_{(a,b)}\vec{u'}_{(b)} \Big| + \sum_{a\in S_0\setminus Q} \Big| \sum_{b\in Q} (T-I)_{(a,b)}\vec{u'}_{(b)} \Big|. \end{aligned} \tag{4.1}$$

For all $b \in Q$ we have $\vec{u'}_{(b)} = \frac{\vec{v}_{(\bar{b})}}{q} > 0$. As established earlier, if $a \in Q$, then $(T-I)_{(a,b)} \leq 0$ and if $a \notin Q$ then $(T-I)_{(a,b)} \geq 0$. Combining this with Lemma 4.7, we have

$$\sum_{a\in Q} \Big| \sum_{b\in Q} (T-I)_{(a,b)}\vec{u'}_{(b)} \Big| = \sum_{a\in S_0\setminus Q} \Big| \sum_{b\in Q} (T-I)_{(a,b)}\vec{u'}_{(b)} \Big|.$$

Continuing with equation (4.1) now gives

$$\begin{aligned} D(\Delta\vec{u'}) &= 2\sum_{a\in Q} \Big| \sum_{b\in Q} (T-I)_{(a,b)}\vec{u'}_{(b)} \Big| = 2\sum_{a\in Q} \Big| \sum_{b\in Q} (T-I)_{(a,b)} \frac{\vec{v}_{(\bar{b})}}{q} \Big| \\ &= 2\sum_{a\in Q} \Big| \sum_{b=a} (T-I)_{(a,b)} \frac{\vec{v}_{(\bar{b})}}{q} + \sum_{b\neq a} (T-I)_{(a,b)} \frac{\vec{v}_{(\bar{b})}}{q} \Big| \\ &= 2\sum_{a\in Q} \Big| \sum_{b=a} (-1) \frac{\vec{v}_{(\bar{b})}}{q} + \sum_{b\neq a} (0) \frac{\vec{v}_{(\bar{b})}}{q} \Big| = 2\sum_{a\in Q} \frac{\vec{v}_{(\bar{b})}}{q} \\ &= \frac{2}{q} \sum_{a\in\mathbb{Z}_N^*} \vec{v}_{(\bar{b})} = \frac{2}{q}(1) = \frac{2}{q}. \end{aligned}$$

□

For a system $S(m/\{2, p_2, ..., p_k\})$ with $N = 2p_2 \cdots p_k$, and prime q coprime to N, if $\vec{w}$ is a real vector with index set $\mathbb{Z}_{Nq}^*$ then define the real vector $\bar{\vec{w}}$ with index set $\mathbb{Z}_N^*$ so that for any $a \in \mathbb{Z}_N^*$ we have $\bar{\vec{w}}_{(a)} = \sum_{b\in S_0 | b\equiv a} \vec{w}_{(b)}$. We then have the following two results:

Lemma 4.9.

$$\overline{P'\vec{w}} = \bar{P}\bar{\vec{w}}.$$

Proof.

$$\begin{aligned}\overline{P'\vec{w}}_{(a)} &= \sum_{b\in S_0|b\equiv a}(P'\vec{w})_{(b)} = \sum_{b\in S_0|b\equiv a}\sum_{c\in S_0}P'_{(b,c)}\vec{w}_{(c)}\\ &= \sum_{c\in S_0}\Big(\vec{w}_{(c)}\sum_{b\in S_0|b\equiv a}P'_{(b,c)}\Big).\end{aligned}$$

Lemma 4.3 and the definition of $\vec{w}$ simplify this to:

$$\begin{aligned}\overline{P'\vec{w}}_{(a)} &= \sum_{c\in S_0}\vec{w}_{(c)}\bar{P}_{(\bar{a},\bar{c})} = \sum_{d\in\mathbb{Z}_N^*}\sum_{c\in S_0|c\equiv d}\vec{w}_{(c)}\bar{P}_{(\bar{a},\bar{c})}\\ &= \sum_{d\in\mathbb{Z}_N^*}\sum_{c\in S_0|c\equiv d}\vec{w}_{(c)}\bar{P}_{(\bar{a},d)} = \sum_{d\in\mathbb{Z}_N^*}\Big(\bar{P}_{(\bar{a},d)}\sum_{c\in S_0|c\equiv d}\vec{w}_{(c)}\Big)\\ &= \sum_{d\in\mathbb{Z}_N^*}\bar{P}_{(\bar{a},d)}\bar{\vec{w}}_{(d)} = (\bar{P}\bar{\vec{w}})_{(a)}.\end{aligned}$$

□

Lemma 4.10.

$$D(\bar{\vec{w}}) \le D(\vec{w}).$$

Proof.

$$\begin{aligned}D(\bar{\vec{w}}) &= \sum_{a\in\mathbb{Z}_N^*}|\bar{\vec{w}}_{(a)}| = \sum_{a\in\mathbb{Z}_N^*}\Big|\sum_{b\in S_0|b\equiv a}\vec{w}_{(b)}\Big|\\ &\le \sum_{a\in\mathbb{Z}_N^*}\sum_{b\in S_0|b\equiv a}|\vec{w}_{(b)}| = \sum_{b\in S_0}|\vec{w}_{(b)}| = D(\vec{w}).\end{aligned}$$

□

The remaining three lemmas will allow us to conclude the proof of the next proposition.

Lemma 4.11. *If $\vec{w}$ is a positive vector such that $\vec{w}_{(a)} \le \frac{1}{q}$ for all $a \in \mathbb{Z}_N^*$ then*

$$(P\vec{w})_{(a)} < \frac{1}{q}\Big(\sum_{b\in\mathbb{Z}_N^*}\bar{P}_{\bar{a},b} + \phi(N)\Big).$$

Proof.

$$\begin{aligned}(P\vec{w})_{(a)} &= \sum_{c\in S_0}P_{(a,c)}\vec{w}_{(c)} \le \sum_{c\in S_0}\Big(P_{(a,c)}\frac{1}{q}\Big) = \frac{1}{q}\Big(\sum_{c\in A}P_{(a,c)} + \sum_{c\notin A}P_{(a,c)}\Big)\\ &\le \frac{1}{q}\Big(\sum_{c\in A}(1) + \sum_{c\notin A}P_{(a,c)}\Big) = \frac{1}{q}\Big(|A| + \sum_{c\notin A}P_{(a,c)}\Big).\end{aligned}$$

Lemma 4.2 states that $|A| = \phi(N)$. Also, if $c \notin A$, then division by q has no effect on c after the "$mx+1$" action and thus $P_{(a,c)} = P'_{(a,c)}$ for all $a \in S_0$.

Using this, and Theorem 4.4 we have

$$(P\vec{w})_{(a)} = \frac{1}{q}\Big(\phi(N) + \sum_{c\notin A} P'_{(a,c)}\Big) \leq \frac{1}{q}\Big(\phi(N) + \sum_{c\in S_0} P'_{(a,c)}\Big)$$
$$= \frac{1}{q}\Big(\phi(N) + \sum_{b\in\mathbb{Z}_N^*}\sum_{c\in S_0|c\equiv b} P'_{(a,c)}\Big) = \frac{1}{q}\Big(\phi(N) + \sum_{b\in\mathbb{Z}_N^*} \bar{P}_{(\bar{a},b)}\Big) \qquad \square$$

Lemma 4.12. *Let M be an n-by-n probability distribution matrix with unique principal eigenvector $\vec{w}$ (where the sum of the entries is 1), and $\{\vec{w_i}\}_{i\in\mathbb{N}}$ be a sequence of vectors in $\mathbb{R}^n$ (whose entries sum to 1) that satisfy*

$$M\vec{w_i} = \vec{w_i} + \vec{\epsilon_i}$$

for some $\vec{\epsilon_i}$ where $D(\vec{\epsilon_i}) \to 0$ as $i \to \infty$. Then,

$$\vec{w_i} \to \vec{w}.$$

Proof. Let $\rho(\vec{v_1}, \vec{v_2}) = D(\vec{v_1} - \vec{v_2})$ be a metric between two vectors in $\mathbb{R}^n$ (the properties of a metric have been confirmed in Lemma 4.6). Define the function $F : \mathbb{R}^n \to \mathbb{R}; F(\vec{w}) = D((M - I)\vec{w})$. Continuity of F under this metric is obvious. Also, $F(\vec{w_i}) = D((M - I)\vec{w_i}) = D(\vec{\epsilon_i})$.

Suppose that for some constant C there is a subsequence $\{\vec{w_{k_i}}\}_{i\in\mathbb{N}} \subset \{\vec{w_i}\}_{i\in\mathbb{N}}$ such that $\rho(\vec{w_{k_i}}, \vec{w}) > C$ for each $i \in \mathbb{N}$.

Let G be the compact set $\{\vec{x} \in [0,1]^n | D(\vec{x}) = 1\}\backslash\{\vec{x} \in \mathbb{R}^n | \rho(\vec{x}, \vec{w}) < C\}$. Clearly, $\vec{w_{k_i}} \in G$ for each $i \in \mathbb{N}$ and so the sequence $\{F(\vec{w_{k_i}})\}_{i\in\mathbb{N}} = \{D(\vec{\epsilon_i})\}_{i\in\mathbb{N}}$ is contained in $F(G)$

Since G is compact, the set $F(G)$ is closed and thus contains all its limits [2, Chapter 6.2]. By the hypothesis, $D(\vec{\epsilon_i}) \to 0$ and so $0 \in F(G)$. Since $\vec{w}$ is a unique principal eigenvector, it is the only solution to $F(\vec{w}) = 0$, thus $\vec{w} \in G$ must be true. But, $\rho(\vec{w}, \vec{w}) = 0 < C$, so $\vec{w} \notin G$, a contradiction.

There is no such C, and therefore $\vec{w_i} \to \vec{w}$. $\square$

Lemma 4.13. *Let $X = \{x_j\}_{j\in\mathbb{N}}$ be a sequence in $\mathbb{R}^+$ and let X_i be either a finite set, or a sequence that converges to 0 for any $i \in \mathbb{Z}^+$. If $X \subset \cup_{i\in\mathbb{Z}^+} X_i$ and $\sup X_i \to 0$ as $i \to 0$ then $x_j \to 0$ as $j \to \infty$.*

Proof. For some $c \in \mathbb{R}$, let $c > 0$. Since $\sup X_i \to 0$, there are only a finite number of indices i such that $x \geq c$ is possible for some $x \in X_i$. Each X_i is either finite or a sequence that converges to 0, so there is at most finitely many $x \in X_i$ such that $x \geq c$. Since a finite union of finite sets is finite, there is at most finitely many $x \in \cup_{i\in\mathbb{Z}^+} X_i$ such that $x \geq c$, and thus at most finitely many $x \in X$ such that $x \geq c$. There must be some M such that $x_j < c$ for all $j > M$ and therefore $x_j \to 0$. $\square$

A few more new notations need to be introduced. First, for any real vector $\vec{w}$ with index set I, let $\vec{w}^+$ be the vector such that $\vec{w}^+_{(i)} = \vec{w}_{(i)}$ when $\vec{w}_{(i)} > 0$ and $\vec{w}^+_{(i)} = 0$ when $\vec{w}_{(i)} \leq 0$ for all $i \in \{1, ..., n\}$. Also, let $\vec{w}^- \in \mathbb{R}^n$ be the

vector such that $\vec{w}^{-}_{(i)} = -\vec{w}_{(i)}$ when $\vec{w}_{(i)} < 0$ and $\vec{w}^{-}_{(i)} = 0$ when $\vec{w}_{(i)} \geq 0$ for all $i \in \{i, ..., n\}$. Basically, $\vec{w}^{+}$ contains the positive components of $\vec{w}$ and $\vec{w}^{-}$ contains the negative components.

Finally, let $\vec{u}$ be the principal eigenvector for P, and let $\vec{\delta} = \vec{u} - \vec{u'}$ (the error between our desired vector $\vec{u}$ and the established vector $\vec{u'}$). The goal of the following proposition is to show that as $q \to \infty$ then $\overline{\vec{\delta}^{+}} \to \overline{\vec{\delta}^{+}}$.

Proposition 4.14. *$\vec{\bar{u}}_{(a)} \to \vec{v}_{(a)}$ as $q \to \infty$ for all $a \in \mathbb{Z}_N^*$.*

Proof. Since $\vec{u}$ is the principal eigenvector for P we have

$$\begin{aligned} P\vec{u} &= \vec{u} \\ P\vec{u'} + P\vec{\delta} &= \vec{u'} + \vec{\delta} \\ (P' + \Delta)\vec{u'} + P\vec{\delta} &= \vec{u'} + \vec{\delta} \\ P'\vec{u'} + \Delta\vec{u'} + P\vec{\delta} &= \vec{u'} + \vec{\delta}. \end{aligned}$$

Recall that u' is the principal eigenvector for P', so $P'\vec{u'} = \vec{u'}$. We now have

$$\begin{aligned} \vec{u'} + \Delta\vec{u'} + P\vec{\delta} &= \vec{u'} + \vec{\delta} \\ \Delta\vec{u'} + P\vec{\delta} &= \vec{\delta} \\ P\vec{\delta} &= \vec{\delta} - \Delta\vec{u'}. \end{aligned} \tag{4.2}$$

Equation (4.2) can be broken into its positive and negative components;

$$\begin{aligned} -(P\vec{\delta})^{-} + (P\vec{\delta})^{+} &= -(\vec{\delta} - \Delta\vec{u'})^{-} + (\vec{\delta} - \Delta\vec{u'})^{+} \\ (P\vec{\delta})^{-} = (\vec{\delta} - \Delta\vec{u'})^{-} \quad &\& \quad (P\vec{\delta})^{+} = (\vec{\delta} - \Delta\vec{u'})^{+}. \end{aligned} \tag{4.3}$$

Let $\vec{e} = [\min\{(P\vec{\delta^{+}})_{(b)}, (P\vec{\delta^{-}})_{(b)}\}]_{b \in S_0}$ (that is, $\vec{e}$ is the overlap in components between $(P\vec{\delta^{+}})$ and $(P\vec{\delta^{-}})$). Then $P\vec{\delta}^{-} = (P\vec{\delta})^{-} + \vec{e}$ and $P\vec{\delta}^{+} = (P\vec{\delta})^{+} + \vec{e}$. Also, $(\vec{\delta} - \Delta\vec{u'})^{-} = (\vec{\delta})^{-} - \vec{w}$ for some $\vec{w}$ with $|\vec{w}_{(b)}| < |(\Delta\vec{u})_{(b)}|$ for all $b \in S_0$ (and clearly, $D(\vec{w}) < D(\Delta\vec{u})$). The first half of equation (4.3) becomes

$$\begin{aligned} P\vec{\delta}^{-} &= \vec{\delta}^{-} + \vec{e} - \vec{w} \\ (P' + \Delta)\vec{\delta}^{-} &= \vec{\delta}^{-} + \vec{e} - \vec{w} \\ P'\vec{\delta}^{-} &= \vec{\delta}^{-} + \vec{e} - \vec{w} - \Delta\vec{\delta}^{-}. \end{aligned} \tag{4.4}$$

In $\mathbb{Z}_N^*$, this is becomes

$$\overline{P'\vec{\delta}^{-}} = \overline{\vec{\delta}^{-}} + \bar{\vec{e}} - \overline{\vec{w}} - \overline{\Delta\vec{\delta}^{-}},$$

and so Lemma 4.9 gives

$$\begin{aligned} \bar{P'}\overline{\vec{\delta}^{-}} &= \overline{\vec{\delta}^{-}} + \bar{\vec{e}} - \overline{\vec{w}} - \overline{\Delta\vec{\delta}^{-}} \\ &= \overline{\vec{\delta}^{-}} + \vec{\beta} \end{aligned} \tag{4.5}$$

for $\vec{\beta} = \bar{\vec{e}} - \bar{\vec{w}} - \overline{\Delta\vec{\delta}^-}$.

Now, according to Lemma 4.6 and equation (4.4) we have

$$\begin{aligned} D(\vec{\delta}^-) \geq D(P\vec{\delta}^-) &= D(\vec{\delta}^- + \vec{e} - \vec{w}) = D(\vec{\delta}^- + \vec{e} - \vec{w}) \\ &\geq D(\vec{\delta}^- + \vec{e}) - D(\vec{w}) = D(\vec{\delta}^-) + D(\vec{e}) - D(\vec{w}) \end{aligned}$$

(the last equality is true since $\vec{\delta}^-$ and $\vec{e}$ are both positive vectors). This results in $D(\vec{e}) \leq D(\vec{w})$. Therefore, by Lemma 4.8 and the previous establishment that $D(\vec{w}) \leq D(\Delta\vec{u})$ we have

$$D(\vec{e}) \leq D(\Delta\vec{u}) = \frac{2}{q}. \tag{4.6}$$

Consider $D(\overline{\Delta\vec{\delta}^-})$. Since $\vec{u}$ is non-negative, it must be true that for each $a \in S_0$, we have $0 \leq \vec{u}_a = \vec{u'}_a + \vec{\delta}_a$, and so $\vec{\delta}_a \geq -\vec{u'}_a = -\frac{\vec{v}_{\bar{a}}}{q}$. So, for each $a \in S_0$ we have $0 \leq (\vec{\delta}^-)_a \leq \frac{\vec{v}_{\bar{a}}}{q}$. Similar to the proof of Lemma 4.8, it is true that $D(\Delta\vec{\delta}^-) \leq \frac{2}{q}$. Lemma 4.10 then gives that $D(\overline{\Delta\vec{\delta}^-}) \leq \frac{2}{q}$.

Combining these results with Lemma 4.6 we get

$$D(\vec{\beta}) \leq D(\bar{\vec{e}}) + D(\overline{\vec{w}^-}) + D(\overline{\Delta\vec{\delta}^-}) \leq \frac{6}{q}. \tag{4.7}$$

Let $J_q = D(\vec{\delta}^-)$ (for each respective q). For all primes q we have that $0 \leq J_q \leq 1$, so if $Y = \{q | q \text{ prime}\} \backslash \{2, p_2, ..., p_k\}$ then we can partition Y into the sets $Y_0 = \{q \in Y | J_q = 0\}$ and $Y_i = \{q \in Y | \frac{1}{i+1} < J_q \leq \frac{1}{i}\}$ for each $i \in \mathbb{N}$.

For any $i > 0$, consider any set Y_i such that Y_i has an infinite number of elements. For each $q \in Y_i$, from Lemma 4.6 and equation (4.7) we have that

$$D\big(\frac{1}{J_q}\vec{\beta}\big) = \frac{1}{J_q} D(\vec{\beta}) < (i+1) D(\vec{\beta}) \leq \frac{6(i+1)}{q}. \tag{4.8}$$

For each $q \in Y_i$, if equation (4.5) is divided by J_q, then along with Lemma 4.12 (we are able to apply this lemma because of Theorem 3.7) and equation (4.8) we have that $\frac{1}{J_q}\overline{\vec{\delta}^-} \to \vec{v}$ (recall that $\vec{v}$ is the principal eigenvector for $\bar{P}$) as $q \to \infty$, or $\overline{\vec{\delta}^-} \to J_q\vec{v}$.

Next, consider the positive components of $\vec{\delta}$. A result of the fact that the sum of the components of both $\vec{u}$ and $\vec{u'}$ is 1 is that $D(\vec{\delta^-}) = D(\vec{\delta^+})$, and therefore for each $q \in Y_i$ we have $D(\vec{\delta^-}) = J_q$. There is also some $\vec{w}$ with $D(\vec{w}) < D(\Delta\vec{u})$ such that the positive counterpart to equation (4.4) is

$$\bar{P}'\overline{\vec{\delta}^+} = \overline{\vec{\delta}^+} + \bar{\vec{e}} - \overline{\vec{w}} - \overline{\Delta\vec{\delta}^+}.$$

In order to show that $\overline{\vec{\delta}^+} \to J_q\vec{v}$ for each $q \in Y_i$, all that remains is to show that $D(\overline{\Delta\vec{\delta}^+}) \to 0$ as $q \to \infty$. First, it will be shown that for each $a \in A$ it must be true that $(\vec{\delta}^+)_{(a)} \to 0$, otherwise the value of $\vec{e}_{(b)}$ will not converge for some $b \in \mathbb{Z}_N^*$ (a contradiction).

As was proved in Chapter 3, $\vec{v}$, the eigenvector for $\bar{P}$ is a fixed non-negative vector. Since $\overrightarrow{\delta^-} \to J_q\vec{v}$, Lemma 4.9 gives us that for all $a \in \mathbb{Z}_N^*$ we have

$$\overrightarrow{(P'\vec{\delta}^-)}_{(a)} = (\bar{P}'\overrightarrow{\vec{\delta}^-})_{(a)} \to J_q(\bar{P}'\vec{v})_{(a)} = J_q\vec{v}_{(a)}.$$

Because $P = P' + \Delta$ and $D(\overrightarrow{\Delta\vec{\delta}^-}) \to 0$ as $q \to \infty$, for every $a \in \mathbb{Z}_N^*$ we have $\overrightarrow{(P\vec{\delta}^-)}_{(a)} \to \overrightarrow{(P'\vec{\delta}^-)}_{(a)}$. If $L = \min\{\vec{v}_{(a)} | a \in \mathbb{Z}_N^*\}$ then for large enough $q \in Y_i$ and for all $a \in \mathbb{Z}_N^*$ we have

$$\overrightarrow{(P\vec{\delta}^-)}_{(a)} > \frac{J_q\vec{v}_{(a)}}{2} \geq \frac{L}{2i}.$$

Let $R = (\vec{\delta}^+)_{(a)}$ for any $a \in A$. From the definition of P and P' it is true that $P\vec{\delta^+} = TP'\vec{\delta^+}$. Recall from the proof of Lemma 4.4 that since $a \in A$ we have $P'_{(b,a)} = \bar{P}_{(\bar{b},\bar{a})}$ for $b \in Q$. By the pigeonhole principle, since the $\phi(N)$ components in any column of $\bar{P}$ sum to 1, there is some $c \in Q$ such that $\bar{P}_{(\bar{c},\bar{a})} \geq \frac{1}{\phi(N)}$. So

$$\begin{aligned}(P'\vec{\delta^+})_{(c)} &= \sum_{b\in S_0} P'_{(c,b)}(\vec{\delta^+})_{(b)} \geq \sum_{b=a\in S_0} P'_{(c,b)}(\vec{\delta^+})_{(b)} = P'_{(c,a)}(\vec{\delta^+})_{(a)} \\ &= \bar{P}_{(\bar{c},\bar{a})}R \geq \frac{R}{\phi(N)}.\end{aligned}$$

According to equation (2.2), if d is the multiplicative order of q in $\mathbb{Z}_N^*$ then for $b, c \in \mathbb{Z}_{Nq}^*$ such that $qb \equiv c \pmod{qN}$ we have $T_{(b,c)} = \frac{q^{d-1}}{q^d-1} \geq \frac{2}{q}$. So

$$\begin{aligned}(P\vec{\delta^+})_{(b)} = (TP'\vec{\delta^+})_{(b)} &= \sum_{a\in S_0} T_{(b,a)}(P'\vec{\delta^+})_{(a)} \\ &\geq \sum_{a=c\in S_0} T_{(b,a)}(P'\vec{\delta^+})_{(a)} = T_{(b,c)}(P'\vec{\delta^+})_{(c)} \\ &\geq \frac{2}{q}\frac{R}{\phi(N)} = \frac{2R}{\phi(N)}\frac{1}{q}.\end{aligned}$$

Recall that $-\frac{\vec{v}_{(\bar{b})}}{q} \leq -(\vec{\delta}^-)_{(b)} \leq 0$. Obviously $0 < \vec{v}_{(\bar{b})} \leq 1$, so we have $0 \leq (\vec{\delta}^-)_{(b)} \leq \frac{1}{q}$. Applying this to Lemma 4.11 gives us that $(P\vec{\delta}^-)_{(b)} \leq \frac{1}{q}(\phi(N) + \sum_{a\in\mathbb{Z}_N^*} \bar{P}_{(\bar{b},a)})$. For any b such that $qb \equiv c \pmod{Nq}$, the ratio of positive components of $(P\vec{\delta})$ over negative components is

$$\frac{(P\vec{\delta}^+)_{(b)}}{(P\vec{\delta}^-)_{(b)}} \geq \frac{\frac{2R}{\phi(N)}\frac{1}{q}}{\frac{1}{q}(\phi(N) + \sum_{a\in\mathbb{Z}_N^*} \bar{P}_{(\bar{b},a)})} = \frac{2R}{\phi(N)\big(\phi(N) + \sum_{a\in\mathbb{Z}_N^*} \bar{P}_{(\bar{b},a)}\big)}.$$

For all such b we have

$$\begin{aligned}\vec{e}_{(b)} &= \min\{(P\vec{\delta^+})_{(b)}, (P\vec{\delta^-})_{(b)}\} \\ &\geq \min\Big\{\frac{2R}{\phi(N)\big(\phi(N)+\sum_{a\in\mathbb{Z}_N^*}\bar{P}_{(\bar{b},a)}\big)}(P\vec{\delta^-})_{(b)}, (P\vec{\delta^-})_{(b)}\Big\} \\ &= \frac{2R}{\phi(N)\big(\phi(N)+\sum_{a\in\mathbb{Z}_N^*}\bar{P}_{(\bar{b},a)}\big)}(P\vec{\delta^-})_{(b)}. \end{aligned} \tag{4.9}$$

The set described by $\{b \in S_0 | qb \equiv c \pmod{qN}\}$ is the same as $\{b \in S_0 | b \equiv cq^{-1}\}$. Recall that if $q \in Y_i$ is large enough then $\overline{(P\vec{\delta^-})}_{(a)} > \frac{L}{2i}$ for all $a \in \mathbb{Z}_N^*$. Specifically, $\overline{(P\vec{\delta^-})}_{(cq^{-1})} > \frac{L}{2i}$. From this and equation (4.9), we have

$$\begin{aligned}\bar{\vec{e}}_{(\overline{cq^{-1}})} &= \sum_{b\in S_0|b\equiv cq^{-1}} \vec{e}_{(b)} \geq \sum_{b\in S_0|b\equiv cq^{-1}} \frac{2R}{\phi(N)\big(\phi(N)+\sum_{a\in\mathbb{Z}_N^*}\bar{P}_{(\bar{b},a)}\big)}(P\vec{\delta^-})_{(b)} \\ &= \frac{2R}{\phi(N)\big(\phi(N)+\sum_{a\in\mathbb{Z}_N^*}\bar{P}_{(\overline{cq^{-1}},a)}\big)} \sum_{b\in S_0|b\equiv cq^{-1}} (P\vec{\delta^-})_{(b)} \\ &= \frac{2R}{\phi(N)\big(\phi(N)+\sum_{a\in\mathbb{Z}_N^*}\bar{P}_{(\overline{cq^{-1}},a)}\big)} \overline{(P\vec{\delta^-})}_{(\overline{cq^{-1}})} \\ &> \frac{2R}{\phi(N)\big(\phi(N)+\sum_{a\in\mathbb{Z}_N^*}\bar{P}_{(\overline{cq^{-1}},a)}\big)} \frac{L}{2i} \\ &= \frac{RL}{\phi(N)i\big(\phi(N)+\sum_{a\in\mathbb{Z}_N^*}\bar{P}_{(\overline{cq^{-1}},a)}\big)}. \end{aligned}$$

Equation (4.6) stated that $D(\bar{\vec{e}}) \to 0$, and since $D(\bar{\vec{e}}) \geq \bar{\vec{e}}_{(\overline{cq^{-1}})}$, it must be true that $\bar{\vec{e}}_{(\overline{cq^{-1}})} \to 0$. We have i, L, $\phi(N)$, and $(\sum_{a\in\mathbb{Z}_N^*}\bar{P}_{(\overline{cq^{-1}},a)})$ all positive constants, so for any $a \in A$ it must be true that $(\vec{\delta^+})_{(a)} = R \to 0$ as $q \to \infty$ in Y_i.

Now, given that $(\vec{\delta^+})_{(a)} = R \to 0$, we can look at $D(\overline{\Delta\vec{\delta^+}})$.

$$\begin{aligned}D(\overline{\Delta\vec{\delta^+}}) &= \sum_{a\in\mathbb{Z}_N^*} |(\overline{\Delta\vec{\delta^+}})_{(a)}| = \sum_{a\in\mathbb{Z}_N^*} \Big|\sum_{b\in S_0|b\equiv a} (\Delta\vec{\delta^+})_{(b)}\Big| \\ &\leq \sum_{a\in\mathbb{Z}_N^*}\sum_{b\in S_0|b\equiv a} \big|(\Delta\vec{\delta^+})_{(b)}\big| = \sum_{a\in\mathbb{Z}_N^*}\sum_{b\in S_0|b\equiv a} \big|\big((T-I)P'\vec{\delta^+}\big)_{(b)}\big| \\ &= \sum_{b\in S_0} \big|\big((T-I)P'\vec{\delta^+}\big)_{(b)}\big|. \end{aligned} \tag{4.10}$$

P' is a non-negative matrix, and $\vec{\delta^+}$ is a non-negative vector, so $P'\vec{\delta^+}$ is a non-negative vector as well. $(T-I)$ has all non-positive entries in the rows corresponding to Q, and non-negative entries in the remaining rows. Thus $(T-I)(P'\vec{\delta^+})$ will have non-positive entries in components corresponding to Q and non-negative entries elsewhere.

By Lemma 4.7, the sum of the entries in $(T-I)P'\vec{\delta}^{+} = \Delta\vec{\delta}^{+}$ is 0. Thus,

$$\sum_{b\in Q}\left|\left((T-I)P'\vec{\delta}^{+}\right)_{(b)}\right| = \sum_{b\notin Q}\left|\left((T-I)P'\vec{\delta}^{+}\right)_{(b)}\right|.$$

So, by splitting S_0 into Q and $S_0\backslash Q$, equation (4.10) becomes

$$\begin{aligned}
D(\overline{\Delta\vec{\delta}^{+}}) &= \sum_{b\in Q}\left|\left((T-I)P'\vec{\delta}^{+}\right)_{(b)}\right| + \sum_{b\notin Q}\left|\left((T-I)P'\vec{\delta}^{+}\right)_{(b)}\right| \\
&= 2\sum_{b\in Q}\left|\left((T-I)P'\vec{\delta}^{+}\right)_{(b)}\right| = 2\sum_{b\in Q}\Big|\sum_{c\in S_0}(T-I)_{(b,c)}(P'\vec{\delta}^{+})_{(c)}\Big| \\
&= 2\sum_{b\in Q}\Big|\sum_{c\in Q}(T-I)_{(b,c)}(P'\vec{\delta}^{+})_{(c)} + \sum_{c\notin Q}(T-I)_{(b,c)}(P'\vec{\delta}^{+})_{(c)}\Big|.
\end{aligned}$$

Recall that $(T-I)_{(b,c)} = 0$ for any $c \notin Q$. Also, $(T-I)_{(b,b)} = -1$ and $(T-I)_{(b,c)} = 0$ when $b, c \in Q$, so

$$\begin{aligned}
D(\overline{\Delta\vec{\delta}^{+}}) &= 2\sum_{b\in Q}\Big|\sum_{c\in Q}(T-I)_{(b,c)}(P'\vec{\delta}^{+})_{(c)} + \sum_{c\notin Q}(0)(P'\vec{\delta}^{+})_{(c)}\Big| \\
&= 2\sum_{b\in Q}\Big|\sum_{c\in Q}(T-I)_{(b,c)}(P'\vec{\delta}^{+})_{(c)}\Big| = 2\sum_{b\in Q}|(-1)(P'\vec{\delta}^{+})_{(b)}| \\
&= 2\sum_{b\in Q}(P'\vec{\delta}^{+})_{(b)} = 2\sum_{b\in Q}\sum_{d\in S_0}P'_{(b,d)}\vec{\delta}^{+}_{(d)} \\
&= 2\sum_{b\in Q}\Big(\sum_{d\in A}P'_{(b,d)}\vec{\delta}^{+}_{(d)} + \sum_{d\notin A}P'_{(b,d)}\vec{\delta}^{+}_{(d)}\Big).
\end{aligned}$$

Recall from the proof of Lemma 4.4 that $P'_{(b,d)} = \bar{P}_{(\bar{b},\bar{d})}$ for $b \in Q$ and $d \in A$, and $P'_{(b,d)} = 0$ for $b \in Q$ and $d \notin A$. So

$$D(\overline{\Delta\vec{\delta}^{+}}) = 2\sum_{b\in Q}\Big(\sum_{d\in A}\bar{P}_{(\bar{b},\bar{d})}\vec{\delta}^{+}_{(d)} + \sum_{d\notin A}(0)\vec{\delta}^{+}_{(d)}\Big) = 2\sum_{b\in Q}\sum_{d\in A}\bar{P}_{(\bar{b},\bar{d})}\vec{\delta}^{+}_{(d)}.$$

It has already been shown that $\vec{\delta}^{+}_{(d)} \to 0$ for each $d \in A$. Since $\bar{P}_{(\bar{b},\bar{d})}$ is fixed for all q, this is a finite sum of values that converge to 0, and thus $D(\overline{\Delta\vec{\delta}^{+}}) \to 0$.

With this established, the proof for negative components can be used to show that $\overline{\vec{\delta}^{+}} \to J_q\vec{v}$ as well. Therefore, for each $a \in \mathbb{Z}_N^*$

$$\begin{aligned}
\bar{\vec{\delta}}_{(a)} &= \sum_{b\in S_0|b\equiv a}\vec{\delta}_{(a)} = \sum_{b\in S_0|b\equiv a}(\vec{\delta}^{+}_{(a)} - \vec{\delta}^{-}_{(a)}) \\
&= \sum_{b\in S_0|b\equiv a}\vec{\delta}^{+}_{(a)} - \sum_{b\in S_0|b\equiv a}\vec{\delta}^{-}_{(a)} \\
&= \overline{\vec{\delta}^{+}}_{(a)} - \overline{\vec{\delta}^{-}}_{(a)} \to J_q\vec{v}_{(a)} - J_q\vec{v}_{(a)} = 0
\end{aligned}$$

From the definition of $\bar{\vec{\delta}}$, we have $\vec{u}_{(a)} \to \vec{v}_{(a)}$ as $q \in Y_i \to \infty$.

If Y is written as the increasing sequence $\{q_j\}_{j\in\mathbb{N}}$ then let $x_j = \bar{\vec{\delta}}_{(a)}$ corresponding to each q_j and let $X = \{x_j\}_{j\in\mathbb{N}}$. Also, let $X_i = \{x_j | q_j \in Y_i\}$ for each $i \in \mathbb{Z}^+$. We can now apply Lemma 4.13 to conclude that as $q \to \infty$ we have $\bar{\vec{\delta}}_{(a)} \to 0$ for each $a \in \mathbb{Z}_N^*$. □

Proposition 4.15. *As $q \to \infty$, the values $\alpha_{2_q}, ..., \alpha_{k_q}$ of $S(m/\{2, p_2, ..., p_k, q\})$ converge to $\alpha_2, ..., \alpha_k$ of $S(m/\{2, p_2, ..., p_k\})$ and $\alpha_{k+1_q} \to 0$.*

Proof. From Lemma 4.1, we can use the values of $\vec{u}$ for the principal eigenvector of $P(S)$. Recall that $\alpha_i = \sum_{a\in\mathbb{Z}_{Nq}^* | p_i \text{ divides } ma+1} \vec{u}_{(a)}$.

First, $\vec{u}_{(a)} \to 0$ as $q \to \infty$. Since $\{a \in \mathbb{Z}_{Nq}^* | p_{k+1} \text{ divides } ma+1\} = A$, we have $\alpha_{k+1} = \sum_{a\in A} \vec{u}_{(a)}$. Lemma 4.2 states that $|A| = \phi(N)$ (constant for all q) and each $\vec{u}_{(a)} \to 0$. Thus α_{k+1} is a finite sum of numbers that converge to 0, and thus α_{k+1} converges to 0.

Consider α_i for $i \in \{2, ..., k\}$. Suppose $ma + 1 \equiv 0 \pmod{p_i}$ for some $a \in \mathbb{Z}_N^*$, and let $b \equiv a$. Clearly $mb + 1 \equiv 0 \pmod{p_i}$ is true. So, we have $\alpha_i = \sum_{a\in\mathbb{Z}_N^* | p_i \text{ divides } ma+1} \vec{v}_{(a)}$ and

$$\begin{aligned}\alpha_{i_q} &= \sum_{b\in\mathbb{Z}_{Nq}^* | p_i \text{ divides } mb+1} \vec{u}_{(b)} = \sum_{a\in\mathbb{Z}_N^* | p_i \text{ divides } ma+1} \Big(\sum_{b\in\mathbb{Z}_{Nq}^* | b\equiv a} \vec{u}_{(b)} \Big) \\ &= \sum_{a\in\mathbb{Z}_N^* | p_i \text{ divides } ma+1} \bar{\vec{u}}_{(a)}.\end{aligned}$$

For each $a \in \mathbb{Z}_N^*$, we have $\bar{\vec{u}}_{(a)} \to \vec{v}_{(a)}$. Because α_{i_q} is a sum of finitely many things, we have $\alpha_{i_q} \to \alpha_i$ □

This brings us to our conclusion:

Theorem 4.16. *If $p_2, ..., p_k, q$ are prime, and m is coprime to q, 2 and each of $p_2, ..., p_k$ then $E(S(m/\{2, p_1, ..., p_k, q\}) \to E(S(m/\{2, p_1, ..., p_k\}))$ as $q \to \infty$.*

Proof. From equation (2.1) and using the previous proposition we have the following:

$$\begin{aligned}E(S(m/\{2, p_1, ..., p_k, q\}) &= \frac{m}{4} \prod_{i=2}^{k+1} \Big(\frac{1}{p_i}\Big)^{\alpha_{i_q} \frac{p_i}{p_i - 1}} \\ &= \frac{m}{4} \prod_{i=2}^{k} \Big(\frac{1}{p_i}\Big)^{\alpha_{i_q} \frac{p_i}{p_i - 1}} \Big(\frac{1}{q}\Big)^{\alpha_{k+1_q} \frac{q}{q-1}} \\ &\to \frac{m}{4} \prod_{i=2}^{k} \Big(\frac{1}{p_i}\Big)^{\alpha_i \frac{p_i}{p_i - 1}} \Big(\frac{1}{q}\Big)^{(0) \frac{q}{q-1}} \\ &= \frac{m}{4} \prod_{i=2}^{k} \Big(\frac{1}{p_i}\Big)^{\alpha_i \frac{p_i}{p_i - 1}} \\ &= E(S(m/\{2, p_1, ..., p_k\}) \end{aligned}$$

□

Chapter 5

Evidence Supporting this Model

5.1 The $E(S) = 1$ threshold

If the calculated expectations are accurate then any system with an expectation less than 1 should have the property that all sequences eventually result in a finite cycle, and any system with expectation greather than one should have the property that some sequences should diverge. Because of this, systems with expectations near the threshold of 1 are investigated in this chapter.

Table 5.27 gives the calculated expectations of several systems. For simplicity, in each case 2 is used as p_1. The 5 systems with expectations closest to 1 from below ($S(11/\{2,3,47\})$, $S(11/\{2,3,53\})$, $S(19/\{2,3,5,11\})$, $S(11/\{2,3,61\})$, $S(23/\{2,3,5,7\})$) and the 5 systems with expectations closest to 1 from above ($S(17/\{2,3,5\})$, $S(5/\{2,7\})$, $S(9/\{2,5,11\})$, $S(11/\{2,3,67\})$, $S(11/\{2,3,59\})$) are investigated regarding divergence.

500 randomly generated numbers (see Table 5.28) were selected, and tested as the initial term for sequences in each of the 10 systems. The sequences were determined until either some term had greater than 10,000 digits, or the remainder of the sequence was cyclic. Tables 5.1 through 5.6 give the results of these tests, where a sequence is considered "divergent" if it eventually reaches a number with greater than 10,000 digits (for these sequences, it is only assumed that the resulting sequences are in fact divergent, but it has not been proven). As expected, for those systems with expectation less than 1, no such sequence was found.

In each block of numbers (the random numbers were seperated into five groups of 100, each group being 8-12 digits long) the highest number attained by any "non-divergent" sequence was recorded. For these sequences, the highest number attained is approximately 2,500 digits long and so it is reasonable to assume that those sequences that attain a number of 10,000 digits are in fact "divergent".

Tables 5.1 through 5.5 suggest the fairly intuitive notion that the closer the expection is to 1 from above, the less likely it is that a sequence will diverge (however a comparison of $S(17/\{2,3,5\})$ and $S(5/\{2,7\})$ seems to contradict this, which could potentially be explained by the choice of smaller divisors having a more significant effect on smaller starting numbers). A second expected trend in the data is that the larger the starting number, the more likely the

sequence is to converge. A hypothesis could be made that as $t_0 \to \infty$, the probability that the sequence beginning with t_0 diverges goes to 1.

Table 5.1: Divergence in $S(17/\{2,3,5\})$ ($E(S) = 1.0384$)

Digits	**Divergent Sequences (ref no.)**	**Tally**	**Highest No.**
8	1, 2, 6, 8, 11, 14, 20, 29, 31, 33, 38, 39, 40, 43, 55, 61, 70, 73, 76, 77, 79, 81, 83, 85, 86, 98, 100	27	$< 1.8 \times 10^{55}$
9	3, 9, 10, 21, 23, 25, 34, 39, 41, 45, 48, 51, 52, 65, 68, 69, 71, 72, 74, 79, 85, 86, 89, 95, 96	25	$< 2.5 \times 10^{55}$
10	8, 9, 10, 12, 13, 14, 15, 21, 23, 40, 45, 48, 52, 55, 58, 60, 61, 64, 67, 68, 73, 78, 87, 88, 97, 99	26	$< 1.2 \times 10^{83}$
11	1, 2, 3, 6, 15, 19, 21, 23, 25, 31, 36, 41, 42, 45, 46, 47, 52, 53, 54, 57, 58, 60, 61, 63, 64, 67, 68, 70, 71, 74, 77, 80, 82, 85, 89, 92, 93, 94, 97, 98, 99, 100	42	$< 3.0 \times 10^{80}$
12	1, 4, 6, 15, 17, 22, 23, 24, 26, 29, 30, 32, 35, 38, 39, 42, 43, 44, 47, 51, 58, 59, 61, 67, 68, 69, 71, 73, 75, 76, 78, 79, 84, 85, 88, 89, 90, 91, 92, 95, 97	41	$< 2.4 \times 10^{31}$
8-12		161	$< 1.2 \times 10^{83}$

Table 5.2: Divergence in $S(5/\{2,7\})$ ($E(S) = 1.0275$)

Digits	**Divergent Sequences (ref no.)**	**Tally**	**Highest No.**
8	1, 2, 4, 5, 6, 7, 8, 11, 12, 14, 15, 16, 18, 19, 22, 27, 28, 29, 30, 31, 32, 33, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 48, 50, 51, 54, 55, 56, 57, 58, 60, 63, 64, 65, 69, 70, 71, 72, 73, 74, 75, 77, 78, 79, 81, 82, 83, 84, 87, 89, 91, 94, 97	64	$< 1.1 \times 10^{47}$
9	7, 10, 13, 14, 15, 19, 20, 21, 23, 24, 27, 28, 31, 33, 35, 36, 38, 41, 44, 45, 47, 48, 53, 54, 55, 57, 63, 65, 66, 68, 70, 74, 75, 77, 78, 79, 82, 83, 86, 87, 90, 91, 93, 97, 98, 99, 100	47	$< 1.3 \times 10^{41}$
10	2, 3, 5, 7, 8, 10, 14, 16, 17, 18, 20, 21, 22, 24, 25, 26, 27, 28, 29, 30, 32, 33, 34, 38, 39, 41, 44, 45, 46, 52, 53, 54, 57, 60, 61, 62, 63, 65, 67, 68, 69, 70, 71, 73, 74, 76, 77, 79, 80, 87, 90, 91, 93, 94, 95, 98, 99	57	$< 1.3 \times 10^{41}$
11	1, 3, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 22, 23, 24, 25, 26, 28, 29, 32, 33, 34, 35, 36, 39, 40, 44, 45, 46, 47, 50, 51, 54, 55, 58, 59, 60, 61, 63, 64, 66, 67, 68, 71, 73, 74, 75, 76, 78, 79, 80, 81, 82, 84, 87, 88, 89, 91, 94, 96, 97, 99, 100	65	$< 2.9 \times 10^{81}$
12	1, 2, 3, 5, 6, 7, 8, 12, 13, 15, 19, 21, 22, 25, 27, 28, 29, 30, 32, 33, 35, 36, 37, 38, 40, 42, 43, 44, 45, 46, 47, 49, 51, 52, 53, 55, 56, 57, 60, 62, 64, 66, 67, 68, 69, 72, 75, 76, 78, 82, 83, 84, 85, 86, 87, 89, 91, 95, 96, 97, 98, 100	62	$< 2.9 \times 10^{81}$
8-12		295	$< 2.9 \times 10^{81}$

Table 5.3: Divergence in $S(9/\{2,5,11\})$ ($E(S) = 1.0182$)

Digits	**Divergent Sequences (ref no.)**	**Tally**	**Highest No.**
8	18, 23, 25, 30, 54, 55, 59, 71, 88, 91, 93, 94	12	$< 5.6 \times 10^{111}$
9	14, 23, 25, 35, 36, 39, 43, 47, 52, 69, 78, 83, 85, 86, 88, 96	16	$< 9.4 \times 10^{77}$
10	7, 12, 13, 27, 28, 32, 33, 35, 39, 40, 43, 46, 49, 58, 72, 78, 79, 81, 84, 90, 100	21	$< 3.1 \times 10^{71}$
11	1, 13, 17, 19, 26, 49, 50, 52, 53, 54, 55, 59, 62, 70, 77, 81, 84, 88, 94, 96, 98, 99	22	$< 3.6 \times 10^{82}$
12	1, 5, 22, 23, 24, 27, 31, 32, 35, 59, 61, 62, 70, 71, 72, 74, 77, 81, 83, 84, 85, 86, 94, 96	24	$< 6.0 \times 10$
8-12		95	$< 5.6 \times 10^{111}$

Table 5.4: Divergence in $S(11/\{2,3,67\})$ ($E(S) = 1.0043$)

Digits	**Divergent Sequences (ref no.)**	**Tally**	**Highest No.**
8	3, 9, 55, 61, 63, 79, 82	7	$< 4.4 \times 10^{101}$
9	13, 36, 61, 63, 64	5	$< 1.1 \times 10^{483}$
10	4, 17, 36, 46, 93	5	$< 8.5 \times 10^{180}$
11	16, 25, 37, 47, 95	5	$< 3.3 \times 10^{173}$
12	8, 25, 26, 28, 54, 59, 81, 86, 100	9	$< 3.6 \times 10^{246}$
8-12		31	$< 1.1 \times 10^{483}$

Table 5.5: Divergence in $S(11/\{2,3,59\})$ ($E(S) = 1.0015$)

Digits	**Divergent Sequences (ref no.)**	**Tally**	**Highest No.**
8	9, 11, 17, 82, 85	5	$< 7.9 \times 10^{841}$
9	39, 85	2	$< 6.0 \times 10^{220}$
10	14, 16	2	$< 4.0 \times 10^{242}$
11	12, 48	2	$< 8.9 \times 10^{1103}$
12	36, 44, 63	3	$< 5.8 \times 10^{2568}$
8-12		14	$< 5.8 \times 10^{2568}$

Table 5.6: Highest Number Attained for Systems with Expectation less than 1

System	**Expectation**	**Highest Number**
$S(11/\{2,3,47\})$	0.9897	$< 1.8 \times 10^{266}$
$S(11/\{2,3,53\})$	0.9931	$< 1.3 \times 10^{446}$
$S(19/\{2,3,5,11\})$	0.9957	$< 8.4 \times 10^{702}$
$S(11/\{2,3,61\})$	0.9994	$< 5.4 \times 10^{1572}$
$S(23/\{2,3,5,7\})$	0.9994	$< 1.7 \times 10^{2523}$

5.2 Occurrence of Divisors

Further support for the proposed eigenvector model for systems can be found in analyzing the individual iterations of each sequence. The construction of the probability distribution matrix was dependent on the notion that, if a number n is divisible by p, then there is an equal probability that $\frac{n}{p} \equiv a \pmod{N}$ for any a such that $ap \equiv n \pmod{N}$.

Tables 5.7 through 5.16 specifically deal with the likelihood of $\frac{n}{p}$ being divisible by p again. Trials were run on the 500 randomly selected numbers from table 5.28 in each of the 10 systems. Each random number had the divisors factored out until the resulting number was coprime to each of the divisors and this resulting number was used as the starting point for each sequence. From there, the system would run until until either the sequence had reached a number less than 1000, or 10000 iterations had been performed[1]. After each iteration, the highest number of divisions by each division that took place were tallied. The results in Tables 5.7 through 5.16 are the percentages for the combined tallies for all 500 starting points.

As stated earlier, if n is divisible by p, then there is a $\frac{1}{p^{k-1}}$ probability that n is divisible by p^k. Thus if n is divisible by p, then there is a $1 - \frac{1}{p} = \frac{p-1}{p}$ probability that n is divisible by p but not p^2, and so there is a $\frac{p-1}{p^k}$ probability that n is divisibly by p^k, but not divisible by p^{k+1}. The expected percentages of tables 5.7 through 5.16 were calculated accordingly.

With very few exceptions, the expected and actual percentages differ by less than five hundredths of a percentage point. It would appear as though the systems are behaving as expected in this regard.

[1] 1000 was chosen to be large enough to avoid the fixed patterns that would occur as the terms in sequences become smaller and repetitive, but small enough to still significant room for sequences to decrease from their initial starting point.

Table 5.7: Expected and Actual Occurrences of Division in $S(17/\{2,3,5\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.945	2^{14}	.006	.005	3^1	36.123	36.128
2^2	25.000	25.023	2^{15}	.003	.003	3^2	12.041	11.999
2^3	12.500	12.498	2^{16}	.002	.002	3^3	4.014	4.034
2^4	6.250	6.257	$2^{\geq 17}$	.002	.002	3^4	1.338	1.347
2^5	3.125	3.152				3^5	.446	.457
2^6	1.563	1.567	5^1	20.542	20.539	3^6	.149	.143
2^7	.781	.774	5^2	4.108	4.127	3^7	.050	.051
2^8	.391	.397	5^3	.822	.805	3^8	.017	.018
2^9	.195	.189	5^4	.164	.164	3^9	.006	.005
2^{10}	.098	.098	5^5	.033	.034	3^{10}	.002	.002
2^{11}	.049	.050	5^6	.007	.007	$3^{\geq 11}$	.001	.001
2^{12}	.024	.024	5^7	.001	.002			
2^{13}	.012	.013	$5^{\geq 8}$	.000	.000			

Table 5.8: Expected and Actual Occurrences of Division in $S(5/\{2,7\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.978	2^{10}	.098	.096	7^1	7.390	7.388
2^2	25.000	24.974	2^{11}	.049	.049	7^2	1.056	1.052
2^3	12.500	12.530	2^{12}	.024	.024	7^3	.151	.153
2^4	6.250	6.239	2^{13}	.012	.012	7^4	.022	.025
2^5	3.125	3.119	2^{14}	.006	.006	7^5	.003	.004
2^6	1.563	1.576	2^{15}	.003	.004	7^6	.000	.001
2^7	.781	.795	2^{16}	.002	.002	$7^{\geq 7}$	.000	.000
2^8	.391	.397	2^{17}	.001	.001			
2^9	.195	.197	$2^{\geq 18}$	.001	.000			

Table 5.9: Expected and Actual Occurrences of Division in $S(9/\{2,5,11\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.930	2^{14}	.006	.006	5^1	23.689	23.717
2^2	25.000	25.050	2^{15}	.003	.005	5^2	4.738	4.726
2^3	12.500	12.515	2^{16}	.002	.001	5^3	.948	.933
2^4	6.250	6.230	2^{17}	.001	.002	5^4	.190	.187
2^5	3.125	3.141	$2^{\geq 18}$	.001	.000	5^5	.038	.040
2^6	1.563	1.565				5^6	.008	.007
2^7	.781	.782	11^1	6.8061	6.8049	5^7	.002	.003
2^8	.391	.394	11^2	.6183	.6201	5^8	.000	.001
2^9	.195	.198	11^3	.0562	.0561	$5^{\geq 9}$	.000	.000
2^{10}	.098	.095	11^4	.0051	.0049			
2^{11}	.049	.051	11^5	.0005	.0006			
2^{12}	.024	.023	11^6	.0000	.0001			
2^{13}	.012	.011	$11^{\geq 7}$	.0000	.0000			

Table 5.10: Expected and Actual Occurrences of Division in $S(11/\{2,3,67\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.937	2^{13}	.012	.012	3^1	38.103	38.159
2^2	25.000	25.050	2^{14}	.006	.005	3^2	12.701	12.681
2^3	12.500	12.554	2^{15}	.003	.002	3^3	4.234	4.215
2^4	6.250	6.227	2^{16}	.002	.001	3^4	1.411	1.405
2^5	3.125	3.125	$2^{\geq 17}$	.002	.000	3^5	.470	.462
2^6	1.563	1.536				3^6	.157	.152
2^7	.781	.790				3^7	.052	.058
2^8	.391	.394	67^1	1.5233	1.5224	3^8	.017	.017
2^9	.195	.203	67^2	.0227	.0238	3^9	.006	.004
2^{10}	.098	.089	67^3	.0003	.0001	3^{10}	.002	.002
2^{11}	.049	.051	67^4	.0000	.0001	3^{11}	.001	.001
2^{12}	.024	.024	$67^{\geq 5}$	.0000	.0000	$3^{\geq 12}$	.000	.000

Table 5.11: Expected and Actual Occurrences of Division in $S(11/\{2,3,59\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.984	2^{13}	.012	.012	3^1	37.947	37.978
2^2	25.000	25.035	2^{14}	.006	.006	3^2	12.649	12.591
2^3	12.500	12.457	2^{15}	.003	.003	3^3	4.216	4.241
2^4	6.250	6.276	2^{16}	.002	.002	3^4	1.405	1.409
2^5	3.125	3.130	2^{17}	.001	.001	3^5	.468	.467
2^6	1.563	1.564	2^{18}	.000	.001	3^6	.156	.155
2^7	.781	.784	$2^{\geq 19}$	.000	.000	3^7	.052	.052
2^8	.391	.388				3^8	.017	.017
2^9	.195	.188	59^1	1.7016	1.7006	3^9	.006	.007
2^{10}	.098	.098	59^2	.0288	.0300	3^{10}	.002	.002
2^{11}	.049	.049	59^3	.0005	.0004	3^{11}	.001	.001
2^{12}	.024	.022	$59^{\geq 4}$	.0000	.0000	$3^{\geq 12}$	.000	.000

Table 5.12: Expected and Actual Occurrences of Division in $S(11/\{2,3,47\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	50.102	2^{13}	.012	.014	3^1	37.981	37.981
2^2	25.000	24.961	2^{14}	.006	.006	3^2	12.660	12.639
2^3	12.500	12.481	2^{15}	.003	.005	3^3	4.220	4.216
2^4	6.250	6.179	2^{16}	.002	.002	3^4	1.407	1.429
2^5	3.125	3.133	$2^{\geq 17}$	.002	.000	3^5	.469	.474
2^6	1.563	1.568				3^6	.156	.158
2^7	.781	.777				3^7	.052	.050
2^8	.391	.393				3^8	.017	.016
2^9	.195	.205	47^1	2.1551	2.1576	3^9	.006	.005
2^{10}	.098	.102	47^2	.0459	.0436	3^{10}	.002	.002
2^{11}	.049	.051	47^3	.0010	.0007	3^{11}	.001	.001
2^{12}	.024	.020	$47^{\geq 4}$	.0000	.0000	$3^{\geq 12}$	.000	.000

Table 5.13: Expected and Actual Occurrences of Division in $S(11/\{2,3,53\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.969	2^{13}	.012	.010	3^1	37.848	37.830
2^2	25.000	25.136	2^{14}	.006	.005	3^2	12.616	12.689
2^3	12.500	12.333	2^{15}	.003	.003	3^3	4.205	4.176
2^4	6.250	6.241	2^{16}	.002	.002	3^4	1.402	1.380
2^5	3.125	3.170	2^{17}	.001	.001	3^5	.467	.476
2^6	1.563	1.594	2^{18}	.000	.001	3^6	.156	.140
2^7	.781	.772	$2^{\geq 19}$	.000	.000	3^7	.052	.050
2^8	.391	.387				3^8	.017	.022
2^9	.196	.201	53^1	1.9847	1.9880	3^9	.006	.007
2^{10}	.098	.102	53^2	.0374	.0337	3^{10}	.002	.001
2^{11}	.049	.051	53^3	.0007	.0012	3^{11}	.001	.001
2^{12}	.024	.023	$53^{\geq 4}$	.0000	.0000	$3^{\geq 12}$	.000	.000

Table 5.14: Expected and Actual Occurrences of Division in $S(19/\{2,3,5,11\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.992	3^1	30.759	30.789	3^7	.042	.039
2^2	25.000	24.951	3^2	10.253	10.214	3^8	.014	.018
2^3	12.500	12.508	3^3	3.418	3.451	3^9	.005	.004
2^4	6.250	6.265	3^4	1.139	1.105	3^{10}	.002	.001
2^5	3.125	3.167	3^5	0.380	.391	3^{11}	.001	.001
2^6	1.563	1.557	3^6	.127	.124	$3^{\geq 12}$	.000	.000
2^7	.781	.797						
2^8	.391	.383						
2^9	.195	.186						
2^{10}	.098	.094						
2^{11}	.049	.048	5^1	20.841	20.814			
2^{12}	.024	.024	5^2	4.168	4.185			
2^{13}	.012	.016	5^3	.834	.837	11^1	9.6997	9.6987
2^{14}	.006	.006	5^4	.167	.172	11^2	.8818	.8873
2^{15}	.003	.003	5^5	.033	.036	11^3	.0802	.0757
2^{16}	.002	.002	5^6	.007	.005	11^4	.0073	.0067
2^{17}	.001	.001	5^7	.001	.001	11^5	.0007	.0012
$2^{\geq 18}$	.001	.000	$5^{\geq 8}$	.000	.000	$11^{\geq 6}$	.0001	.0000

Table 5.15: Expected and Actual Occurrences of Division in $S(11/\{2,3,61\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.933	2^{13}	.012	.014	3^1	38.104	38.037
2^2	25.000	25.045	2^{14}	.006	.006	3^2	12.701	12.741
2^3	12.500	12.471	2^{15}	.003	.003	3^3	4.234	4.243
2^4	6.250	6.287	2^{16}	.002	.001	3^4	1.411	1.424
2^5	3.125	3.105	2^{17}	.001	.001	3^5	.470	.466
2^6	1.563	1.583	2^{18}	.000	.001	3^6	.157	.167
2^7	.781	.799	$2^{\geq 19}$	.000	.000	3^7	.052	.053
2^8	.391	.387				3^8	.017	.016
2^9	.195	.192	61^1	1.6488	1.6454	3^9	.006	.006
2^{10}	.098	.098	61^2	.0270	.0299	3^{10}	.002	.001
2^{11}	.049	.049	61^3	.0004	.0009	3^{11}	.001	.001
2^{12}	.024	.025	$61^{\geq 4}$	.0000	.0000	$3^{\geq 12}$	.000	.000

Table 5.16: Expected and Actual Occurrences of Division in $S(23/\{2,3,5,7\})$

Div	exp %	Act %	Div	exp %	Act %	Div	exp %	Act %
2^1	50.000	49.962	3^1	36.069	36.044	3^6	.148	.145
2^2	25.000	24.943	3^2	12.023	12.058	3^7	.049	.047
2^3	12.500	12.556	3^3	4.008	3.994	3^8	.016	.016
2^4	6.250	6.224	3^4	1.336	1.350	3^9	.005	.004
2^5	3.125	3.125	3^5	.445	.441	3^{10}	.002	.003
2^6	1.563	1.613				$3^{\geq 11}$	.001	.001
2^7	.781	.788						
2^8	.391	.387						
2^9	.195	.206						
2^{10}	.098	.099	5^1	18.251	18.280			
2^{11}	.049	.051	5^2	3.650	3.639	7^1	14.976	14.974
2^{12}	.024	.025	5^3	.730	.721	7^2	2.139	2.141
2^{13}	.012	.011	5^4	.146	.137	7^3	.306	.308
2^{14}	.006	.005	5^5	.029	.029	7^4	.044	.042
2^{15}	.003	.003	5^6	.006	.006	7^5	.006	.005
2^{16}	.002	.002	5^7	.001	.001	7^6	.001	.001
$2^{\geq 17}$	.002	.001	$5^{\geq 8}$	.000	.000	$7^{\geq 7}$	.000	.000

5.3 Occurrence of Residues

Finally, the principal eigenvectors were tested. The 500 randomly generated numbers were run through the same test as the previous section; however this time the residues modulo $p_1 \cdots p_k$ were tallied for each system $S(m/\{p_1, ..., p_k\})$ instead of the number of divisions. Again, the expected and actual percentages are significantly close, suggesting that this model is likely appropriate.

Table 5.17: Expected and Actual Occurrences for Residues in $S(17/\{2, 3, 5\})$

Res	exp %	Act %	Res	exp %	Act %	Res	exp %	Act %
1	14.996	14.987	13	9.729	9.717	23	13.223	13.204
7	13.443	13.444	17	12.170	12.233	29	10.326	10.347
11	10.035	10.029	19	16.077	16.038			

Table 5.18: Expected and Actual Occurrences for Residues in $S(5/\{2, 7\})$

Res	exp %	Act %	Res	exp %	Act %	Res	exp %	Act %
1	15.827	15.859	5	22.302	22.302	11	8.633	8.622
3	20.144	20.161	9	10.072	10.119	13	23.022	22.937

Table 5.19: Expected and Actual Occurrences for Residues in $S(9/\{2, 5, 11\})$

Res	Exp %	Act %	Res	Exp %	Act %	Res	Exp %	Act %
1	3.1752	3.2983	41	2.6844	3.1351	79	2.2477	2.4142
3	1.4996	1.5039	43	1.7844	1.7128	81	3.0690	3.3052
7	3.2776	3.1746	47	2.9884	2.5763	83	1.8999	2.0900
9	2.3722	2.3134	49	2.4331	2.3252	87	3.1017	2.9552
13	1.9014	2.0048	51	3.2383	2.7756	89	2.2533	2.4266
17	1.6037	1.7094	53	2.0513	1.7959	91	2.5029	2.5397
19	2.3570	2.2552	57	3.3360	3.3049	93	1.9134	1.7985
21	2.9355	2.8396	59	2.5073	2.5026	97	3.1807	3.1757
23	2.0112	2.0395	61	2.0955	2.1248	101	3.2459	3.3120
27	2.9892	3.0151	63	2.0107	1.9487	103	1.7976	2.0036
29	1.9870	2.1065	67	3.3156	3.1878	107	2.5435	3.2354
31	3.3825	3.1551	69	2.4423	2.3248	109	2.2143	1.9358
37	3.2932	3.3147	71	3.3004	3.1290			
39	1.4078	1.5635	73	1.6490	1.6709			

Table 5.20: Expected and Actual Occurrences for Residues in $S(11/\{2,3,67\})$

Res	Exp %	Act %	Res	Exp %	Act %	Res	Exp %	Act %
1	.89434	.89504	137	.66349	.65522	269	.66690	.66736
5	.65235	.67151	139	.86943	.87190	271	.86653	.86993
7	.80489	.82873	143	.65949	.64962	275	.65165	.67473
11	.66428	.66560	145	.88150	.88726	277	.88191	.87366
13	.87939	.87387	149	.66535	.67670	281	.64011	.64910
17	.50668	.49614	151	.89777	.89255	283	.88454	.88643
19	.88445	.88041	155	.62136	.62409	287	.66643	.67649
23	.66127	.66477	157	.88422	.86723	289	.87889	.87729
25	.86505	.86588	161	.64157	.63312	293	.66143	.65709
29	.59798	.58341	163	.83219	.83547	295	.80519	.79241
31	.86711	.85478	167	.65243	.64536	299	.65546	.64630
35	.65568	.65948	169	.89082	.88539	301	.87917	.87345
37	.87850	.88477	173	.66468	.67618	305	.62242	.62793
41	.61865	.62658	175	.84589	.85924	307	.88686	.89867
43	.88814	.88445	179	.66711	.68282	311	.66326	.66477
47	.60347	.60365	181	.86018	.86194	313	.89497	.91662
49	.86410	.86723	185	.66895	.66466	317	.65427	.66134
53	.65960	.66031	187	.88290	.86640	319	.88891	.90033
55	.88440	.87750	191	.65016	.65761	323	.66337	.65896
59	.66339	.66031	193	.88622	.90324	325	.85847	.85488
61	.89108	.89556	197	.66636	.65584	329	.66448	.66103
65	.66420	.66134	199	.89491	.89660	331	.88193	.89711
71	.66614	.65543	203	.66874	.66944	337	.88827	.88435
73	.88229	.89473	205	.89127	.89037	341	.65602	.65148
77	.66579	.66197	209	.66624	.66456	343	.88734	.87086
79	.88114	.87844	211	.88166	.88788	347	.65686	.65190
83	.65700	.64765	215	.63207	.64526	349	.85983	.87252
85	.86535	.87812	217	.88753	.90521	353	.64646	.65916
89	.64419	.65273	221	.65710	.67390	355	.85817	.87273
91	.87420	.86235	223	.88593	.90241	359	.66703	.63675
95	.59605	.58175	227	.65784	.65875	361	.86705	.85384
97	.88015	.85727	229	.81514	.82375	365	.66703	.66352
101	.67094	.66062	233	.65283	.64121	367	.86705	.86816
103	.87131	.87273	235	.56219	.56722	371	.64325	.63644
107	.65883	.65190	239	.65930	.64827	373	.88627	.90469
109	.81164	.80237	241	.86912	.86515	377	.67256	.66176
113	.65308	.65387	245	.66278	.65169	379	.85502	.83651
115	.85433	.86194	247	.88132	.87325	383	.64025	.63395
119	.66065	.66041	251	.66373	.67369	385	.88507	.86910
121	.83340	.81804	253	.86790	.88259	389	.64402	.63395
125	.65396	.65937	257	.52430	.53163	391	.74841	.73679
127	.88423	.89006	259	.85575	.85197	395	.66028	.66549
131	.66510	.66861	263	.64991	.66300	397	.87980	.89317
133	.87147	.87013	265	.89305	.88279	401	.65814	.65283

Table 5.21: Expected and Actual Occurrences for Residues in $S(11/\{2,3,59\})$

Res	Exp %	Act %	Res	Exp %	Act %	Res	Exp %	Act %
1	.9972	.9837	121	.9582	.9631	239	.7057	.6956
5	.6822	36670	125	.7648	.7780	241	.9372	.9255
7	1.0080	1.0111	127	.9652	.9539	245	.7425	.7446
11	.7638	.7643	131	.7283	.7343	247	1.0043	1.0134
13	1.0015	1.0040	133	1.0137	.9926	251	.5760	.5769
17	.7610	.7607	137	.7623	.7662	253	.9769	.9791
19	1.0062	1.0321	139	1.0050	1.0148	257	.7495	.7637
23	.7144	.7153	143	.7595	.7417	259	.9590	.9585
25	1.0158	1.0129	145	1.0060	.9934	263	.7584	.7544
29	.7380	.7540	149	.7397	.7377	265	.9899	.9899
31	.9865	.9867	151	1.0129	1.0133	269	.7634	.7716
35	.7647	.7729	155	.7638	.7516	271	1.0188	1.0047
37	.8884	.9026	157	1.0146	1.0149	275	.7603	.7680
41	.7425	.7653	161	.7639	.7635	277	.9786	.9825
43	1.0111	.9906	163	.9978	.9962	281	.7458	.7599
47	.7518	.7630	167	.7585	.7598	283	1.0035	.9984
49	.9964	1.0067	169	1.0105	1.0100	287	.76291	.7655
53	.7623	.7569	173	.7631	.7475	289	1.0002	1.0070
55	1.0159	1.0290	175	1.0084	1.0307	293	.7663	.7766
61	.9955	1.0273	179	.7292	.7266	299	.7626	.7587
65	.6964	.6985	181	.9816	.9797	301	.9164	.9054
67	1.0066	1.0041	185	.7603	.7506	305	.6007	.5922
71	.6992	.7083	187	.8417	.8508	307	1.0013	1.0127
73	1.0157	1.0102	191	.7471	.7478	311	.7365	.7381
77	.7442	.7452	193	.9948	.9934	313	1.0009	.9864
79	1.0129	1.0055	197	.7586	.7552	317	.7544	.7515
83	.7528	.7493	199	1.0054	1.0107	319	.8821	.8723
85	.9351	.9322	203	.7655	.7717	323	.7673	.7636
89	.7601	.7601	205	.9742	.9761	325	.6327	.6103
91	.9639	.9702	209	.7282	.7243	329	.7450	.7426
95	.7546	.7558	211	1.0068	1.0145	331	.9891	.9908
97	1.0034	.9874	215	.7373	.7236	335	.7564	.7416
101	.7719	.7696	217	.9950	.9911	337	1.0066	1.0248
103	.9988	.9934	221	.7547	.7493	341	.7698	.7599
107	.6788	.6842	223	1.0201	1.0126	343	.9840	.9948
109	.9957	1.0084	227	.7487	.7712	347	.7579	.7593
113	.7388	.7527	229	1.0072	1.0114	349	.9950	.9921
115	1.0106	.9948	233	.7544	.7560	353	.7627	.7587
119	.7545	.7358	235	.9749	.9570			

Table 5.22: Expected and Actual Occurrences for Residues in $S(11/\{2,3,47\})$

Res	Exp %	Act %	Res	Exp %	Act %	Res	Exp %	Act %
1	1.2577	1.2195	97	1.2810	1.2720	191	.9099	.9344
5	.8982	.8843	101	.9369	.9274	193	1.2006	1.2150
7	1.2362	1.2503	103	1.2695	1.2702	197	.9596	.9444
11	.9621	.9498	107	.9415	.9274	199	1.2713	1.2686
13	1.2329	1.2557	109	1.2746	1.2657	203	.9692	.9530
17	.9440	.9779	113	.9594	.9286	205	1.2084	1.2229
19	1.2801	1.2695	115	1.1846	1.2110	209	.9784	.9876
23	.9202	.9087	119	.9623	9595	211	1.2202	1.2166
25	1.2377	1.2309	121	1.2492	1.2455	215	.9299	.9227
29	.9690	.9424	125	.9554	.9462	217	1.2878	1.2675
31	1.2762	1.2810	127	1.2326	1.2361	221	.9427	.9378
35	.9396	.9401	131	.9617	.9690	223	1.2412	1.2329
37	1.2756	1.2976	133	1.2558	1.2743	227	.9576	.9575
41	.9546	.9575	137	.9535	.9774	229	1.2653	1.2743
43	1.1582	1.1603	139	1.2850	1.2738	233	.9069	.9207
49	1.2280	1.2261	143	.9227	.9161	239	.8611	.8397
53	.9591	.9849	145	1.1845	1.1879	241	1.1569	1.1680
55	1.0566	1.0568	149	.7509	.7717	245	.9733	.9541
59	.7274	.7323	151	1.2884	1.3043	247	1.2593	1.2478
61	1.2763	1.2578	155	.9473	.9378	251	.9650	.9729
65	.9665	.9618	157	1.2637	1.2734	253	1.2706	1.2862
67	1.2793	1.2593	161	.9700	.9740	257	.9721	.9582
71	.9527	.9383	163	1.2935	1.3197	259	.7876	.7902
73	1.2358	1.2507	167	.9312	.9130	263	.9667	.9769
77	.9459	.9161	169	1.2510	1.2569	265	1.2681	1.2731
79	1.2631	1.2327	173	.9185	.9360	269	.8513	.8693
83	.9491	.9537	175	1.2129	1.1917	271	1.2861	1.2808
85	1.2886	1.3172	179	.9806	.9582	275	.9436	.9523
89	.9683	.9394	181	1.2739	1.3113	277	1.2872	1.2912
91	1.2828	1.2903	185	.9668	.9772	281	.9713	.9616
95	.9471	.9274	187	1.2029	1.1922			

Table 5.23: Expected and Actual Occurrences for Residues in $S(11/\{2,3,53\})$

Res	Exp %	Act %	Res	Exp %	Act %	Res	Exp %	Act %
1	1.0946	1.1174	109	1.0640	1.0573	215	.7910	.7956
5	.8529	.8816	113	.8436	.8667	217	1.1089	1.0867
7	1.1185	1.1534	115	.9241	.9284	221	.6670	.6662
11	.8355	.8211	119	.8550	.8582	223	1.1237	1.1283
13	1.1357	1.1318	121	1.1157	1.1136	227	.8508	.8472
17	.8516	.8456	125	.8486	.8454	229	1.1009	1.1046
19	1.1329	1.1311	127	1.1129	1.1216	233	.8320	.8351
23	.8441	.8465	131	.8043	.8084	235	1.1228	1.1260
25	1.1286	1.1075	133	.6929	.6772	239	.8333	.8491
29	.8294	.8801	137	.7497	.7567	241	1.0947	1.1152
31	1.0438	1.0401	139	1.1183	1.1271	245	.8478	.8445
35	.8337	.8199	143	.8489	.8202	247	1.0201	1.0295
37	1.1215	1.1306	145	1.1086	1.1205	251	.8569	.8825
41	.8306	.7975	149	.8526	.8607	253	1.1158	1.1134
43	1.1261	1.1603	151	1.1294	1.1134	257	.8491	.8402
47	.8502	.8218	155	.8516	.8413	259	1.1247	1.0953
49	1.1212	1.1170	157	1.1293	1.1130	263	.8545	.8570
55	1.1198	1.1117	161	.8363	.8524	269	.8353	.8453
59	.8320	.8143	163	1.0980	1.1236	271	1.1271	1.1016
61	1.1082	1.1036	167	.8455	.8376	275	.8025	.7779
65	.8655	.8993	169	1.1263	1.1181	277	1.0889	1.0719
67	1.1012	1.0636	173	.8349	.8211	281	.8075	.8093
71	.8478	.8646	175	1.1017	1.0782	283	1.1253	1.1326
73	1.0295	1.0278	179	.8611	.8758	287	.8429	.8429
77	.8547	.8884	181	1.0938	1.0988	289	1.1419	1.1352
79	1.1241	1.1530	185	.8431	.8441	293	.8085	.8198
83	.8375	.8436	187	1.0906	1.0683	295	1.1175	1.0864
85	1.0343	1.0502	191	.7842	.7713	299	.8455	.8582
89	.8582	.8532	193	1.1220	1.1248	301	1.1328	1.0962
91	1.1268	1.1455	197	.8559	.8589	305	.6380	.6320
95	.8167	.8278	199	1.1330	1.1597	307	1.0832	1.0934
97	1.0949	1.0629	203	.8039	.8205	311	.8256	.8198
101	.8569	.8805	205	1.1001	1.0901	313	1.1226	1.0828
103	1.0301	1.0241	209	.8418	.8395	317	.8208	.8120
107	.8295	.8248	211	1.0999	1.1111			

Table 5.24: Expected and Actual Occurrences for Residues in $S(19/\{2,3,5,11\})$

Res	Exp %	Act %	Res	Exp %	Act %	Res	Exp %	Act %
1	1.5251	1.4997	109	1.5668	1.5525	227	1.1739	1.1979
7	1.6422	1.6384	113	1.0030	.9936	229	1.6233	1.6136
13	.7413	.7301	119	1.0259	1.0419	233	1.1724	1.1852
17	1.1798	1.1703	127	.8169	.8051	239	1.0265	1.0535
19	1.5230	1.5448	131	1.1150	1.1323	241	1.5259	1.5230
23	1.3653	1.3835	133	1.0562	1.0482	247	1.5016	1.5078
29	1.0450	1.0311	137	1.3575	1.3470	251	1.2450	1.2504
31	1.6470	1.6345	139	1.3946	1.3785	257	1.3202	1.3203
37	1.6261	1.6497	149	.9985	1.0008	259	1.0662	1.0378
41	1.0905	1.0830	151	1.3710	1.3828	263	1.1982	1.1869
43	1.0200	1.0258	157	1.6138	1.6155	269	1.1376	1.1222
47	1.0847	1.1025	161	1.1712	1.1794	271	1.4354	1.4590
49	1.5560	1.5725	163	1.0558	1.0628	277	1.5000	1.4720
53	1.2980	1.2816	167	1.1470	1.1443	281	1.1423	1.1554
59	1.0816	1.1030	169	1.5699	1.5795	283	.9934	.9854
61	.8192	.8198	173	1.2794	1.2787	287	1.1773	1.2025
67	1.6027	1.6011	179	1.0872	1.0499	289	1.4086	1.4186
71	1.2476	1.2513	181	1.5894	1.5910	293	1.2922	1.2963
73	.8493	.8383	191	1.0842	1.0785	299	.8782	.8683
79	1.3377	1.3088	193	.9760	.9888	301	1.6598	1.6470
83	1.1997	1.1999	197	1.1586	1.1547	307	1.6163	1.5946
89	.9370	.9446	199	1.4372	1.4350	311	.84457	.8671
91	1.5101	1.5271	203	1.3630	1.3657	313	1.0320	1.0335
97	1.7656	1.7836	211	1.6323	1.6182	317	1.2354	1.2561
101	1.2105	1.1790	217	1.3051	1.3018	323	1.2721	1.2792
103	1.0030	1.0119	221	1.1679	1.1729	329	.9366	.9229
107	1.2888	1.2968	223	1.0452	1.0313			

Table 5.25: Expected and Actual Occurrences for Residues in $S(11/\{2,3,61\})$

Res	Exp %	Act %	Res	Exp %	Act %	Res	Exp %	Act %
1	.9826	.9937	125	.7308	.7254	245	.7317	.7276
5	.7237	.7121	127	.9818	.9862	247	.9784	.9968
7	.9542	.9494	131	.7260	.7034	251	.7168	.7243
11	.7254	.7154	133	.9618	.9602	253	.9528	.9746
13	.9677	.9762	137	.7329	.7452	257	.7140	.7162
17	.6608	.6545	139	.9245	.9125	259	.9727	.9662
19	.9388	.9385	143	.7381	.7342	263	.7161	.7106
23	.7344	.7300	145	.8928	.8650	265	.9593	.9724
25	.9759	.9920	149	.7244	.7394	269	.7344	.7245
29	.7292	.7127	151	.9758	.9779	271	.9760	1.0096
31	.6115	.5945	155	.7362	.7383	275	.7309	.7317
35	.7179	.7288	157	.9731	.9613	277	.9436	.9489
37	.8944	.8904	161	.7091	.7204	281	.7280	.7553
41	.7263	.7346	163	.9840	.9817	283	.9417	.9301
43	.9641	.9649	167	.7339	.7461	287	.7156	.7158
47	.7093	.7003	169	.9703	.9799	289	.9764	.9802
49	.9800	1.0015	173	.5745	.5619	293	.6917	.6877
53	.7083	.7123	175	.9603	.9580	295	.8164	.8072
55	.9635	.9761	179	.6662	.6885	299	.7326	.7267
59	.6982	.6916	181	.9488	.9523	301	.9095	.8853
65	.7343	.7399	185	.7417	.7398	307	.9708	.9771
67	.9892	.9634	187	.9841	.9889	311	.7362	.7437
71	.7238	.7040	191	.7355	.7315	313	.9820	1.0148
73	.9730	.9758	193	.9539	.9519	317	.7353	.7445
77	.7266	.7217	197	.7172	.7171	319	.9684	.9707
79	.9604	.9431	199	.9814	.9914	323	.7357	.7548
83	.7204	.7191	203	.6841	.6890	325	.9538	.9480
85	.9787	1.0075	205	.9738	.9697	329	.7244	.7282
89	.6958	.6963	209	.7053	.7119	331	.9400	.9426
91	.9720	.9782	211	.9411	.9115	335	.7301	.7373
95	.7251	.7388	215	.7292	.7342	337	.9660	.9566
97	.9796	.9701	217	.9406	.9344	341	.7241	.7284
101	.7138	.7047	221	.7264	.7208	343	.9771	.9439
103	.9906	.9798	223	.8846	.9012	347	.6929	.6767
107	.5523	.5420	227	.7351	.7334	349	.9735	.9664
109	.9619	.9686	229	.9801	.9868	353	.7293	.7105
113	.7176	.7344	233	.7189	.7309	355	.9716	.9632
115	.9660	.9620	235	.9521	.9690	359	.7326	.7159
119	.7196	.7086	239	.6563	.6535	361	.9014	.8888
121	.9688	.9902	241	.9735	.9637	365	.7200	.7102

Table 5.26: Expected and Actual Occurrences for Residues in $S(23/\{2,3,5,7\})$

Res	Exp %	Act %	Res	Exp %	Act %	Res	Exp %	Act %
1	2.6144	2.6120	71	2.0251	2.0468	143	2.2849	2.2957
11	1.8404	1.8959	73	1.9797	1.9974	149	1.8478	1.8283
13	1.4270	1.4446	79	2.6497	2.6495	151	1.6125	1.5920
17	2.1123	2.0861	83	1.9523	1.9461	157	2.5821	2.5809
19	2.8056	2.8401	89	1.6456	1.6431	163	1.8009	1.8054
23	1.7093	1.6731	97	1.9812	1.9930	167	1.9100	1.9241
29	1.9745	2.0122	101	1.6172	1.5967	169	2.5721	2.5208
31	2.4670	2.4563	103	1.6948	1.6729	173	1.9537	1.9523
37	2.6621	2.6591	107	1.9392	1.9278	179	1.7728	1.7516
41	1.9652	1.9917	109	1.9463	1.9764	181	2.5073	2.4962
43	1.6622	1.6195	113	2.3006	2.3239	187	2.6786	2.6429
47	1.9446	1.9675	121	2.5091	2.5156	191	1.4267	1.4160
53	2.1960	2.1828	127	2.5957	2.5888	193	1.9014	1.8981
59	1.8105	1.8280	131	1.7385	1.7363	197	2.2110	2.2192
61	2.7395	2.7299	137	2.1670	2.1428	199	2.6250	2.6314
67	1.8310	1.8356	139	2.3462	2.3467	209	1.4635	1.5067

5.4 Other Data

Table 5.27: Multiplicative Expectations for some Systems

System	Exp.	System	Exp.	System	Exp.
$S(3/\{2\})$	0.75	$S(7/\{2,3\})$	0.9052	$S(11/\{2,3\})$	1.0724
		$S(7/\{2,5\})$	0.9642	$S(11/\{2,3,17\})$	0.9190
$S(5/\{2\})$	1.25	$S(7/\{2,11,13\})$	1.1155	$S(11/\{2,3,19\})$	0.9031
$S(5/\{2,3\})$	0.4875	$S(7/\{2,11,17\})$	1.1711	$S(11/\{2,3,23\})$	0.9386
$S(5/\{2,7\})$	1.0275			$S(11/\{2,3,29\})$	0.9550
$S(5/\{2,7,11\})$	0.7546	$S(9/\{2,5,11\})$	1.0182	$S(11/\{2,3,31\})$	0.9560
$S(5/\{2,7,13\})$	0.8419			$S(11/\{2,3,37\})$	0.9655
$S(5/\{2,7,17\})$	0.8161	$S(13/\{2,3,5\})$	1.0845	$S(11/\{2,3,41\})$	0.9764
$S(5/\{2,7,19\})$	0.8433			$S(11/\{2,3,43\})$	0.9784
$S(5/\{2,7,23\})$	0.8672	$S(17/\{2,3,5\})$	1.0384	$S(11/\{2,3,47\})$	0.9897
$S(5/\{2,7,29\})$	0.9104			$S(11/\{2,3,53\})$	0.9931
$S(5/\{2,7,31\})$	0.8889	$S(19/\{2,3,5,7\})$	0.9592	$S(11/\{2,3,59\})$	1.0015
$S(5/\{2,11\})$	0.9263	$S(19/\{2,3,5,11\})$	0.9957	$S(11/\{2,3,61\})$	0.9994
$S(5/\{2,11,13\})$	0.7688	$S(19/\{2,3,5,13\})$	1.0727	$S(11/\{2,3,67\})$	1.0043
$S(5/\{2,11,17\})$	0.7528				
$S(5/\{2,11,19\})$	0.7728	$S(23/\{2,3,5,7\})$	0.9994		

Table 5.28: Random Numbers Used in Trials

Ref #	8 Digits	9 Digits	10 Digits	11 Digits	12 Digits
1	43949058	133751076	5840371500	73715876729	712999543523
2	57237679	586158240	8010929594	65700862943	245330984447
3	56764175	467287522	6491108036	32424170465	376587456075
4	15883987	153610815	5112460519	25235196453	641902908204
5	84600232	879850007	3816384844	27988963610	374651966999
6	95132796	319106125	5144164697	44344539876	406449767634
7	44637620	155540012	9463631539	17412421905	850409669815
8	36107037	225500149	8732145756	95818212663	902454155507
9	20607915	168378689	7106418225	53421525586	434796455572
10	47522486	868172695	9415955883	83497475450	772869014214
11	14922351	532668526	1581869302	72877304839	440895669155
12	61780436	505135326	5161255391	52427536557	839457647004
13	62449056	437262560	6244301281	59407854984	212155351554
14	56403365	235838395	1809094426	64966684858	942468887962
15	49054505	996998889	9451185402	75976255360	522605526665
16	79209560	554958197	8412421905	32385044556	960696306908
17	58557997	301029038	4427838553	68760991782	164544616043
18	22870850	190777717	2275731771	21770990285	260846663823
19	90377252	915637919	1020544909	71942394930	727488467546
20	63530478	750994542	5777998714	96646091147	232783285421
21	76253611	801327918	9067798189	88606118334	119182685523
22	36965090	632834019	4427077306	43489062233	996485642968

Continued on next page

Table 5.28 – continued from previous page

Ref #	8 Digits	9 Digits	10 Digits	11 Digits	12 Digits
23	69871636	830798472	6205175372	19949508400	936386069679
24	86951880	869381295	8221384230	82466529986	197309133939
25	12831035	310675943	3039073006	27820308836	702222289407
26	43751076	724983095	1746745227	52924197337	796005861184
27	93505056	686128038	4747053250	52184753306	375130015257
28	63610815	604386587	1640439652	14832623175	962790603924
29	94888397	751006053	9564458969	94884659950	814721677141
30	65540012	182648824	8825014938	16402031176	792355458282
31	78378689	262087183	5832623175	98749509928	392167296340
32	59739450	675390759	7402031176	36310525699	459387387685
33	40015342	680542173	3850164008	58147481356	525549978857
34	95293656	998599952	9809907465	87529384201	633990756471
35	12482142	801311587	9746448575	70286056127	702882754492
36	78827104	177594039	2755486969	46115225337	502854435326
37	11620667	298358220	4468319344	59211688700	113642900126
38	89601089	455822512	8326244625	55043765555	718873478963
39	62305013	523966005	9602039667	47828057712	233400028636
40	76811310	172387746	7253613363	52961778035	444829638290
41	43506413	150986366	4323948758	42830562320	167499645464
42	20331551	434138857	7759224824	33433482547	480076868136
43	65166217	466604856	4765644424	82043425494	340110681519
44	96533896	654334954	4471087299	16759224824	965025968658
45	40239278	871925675	9666272892	99664990344	796074080969
46	69709832	280220195	8820451619	47830825667	239049672077
47	86458215	686491243	7790157226	87385749628	185248995821
48	98112183	517082766	1678852156	35000320803	642977065094
49	59257126	558538714	4477783405	26922489097	670667848839
50	92600807	108479921	6227996711	41837160257	782887092972
51	92648824	760382807	9192069084	16790157226	879083730166
52	37869455	106862945	8939108714	96578198076	938945695809
53	48519847	153853750	8640307487	73401152795	409422465404
54	53671261	224776206	8280969794	53938185730	550355304119
55	40222947	257138152	8214771064	30657652589	998424235844
56	87594039	523909157	2685003584	40015471722	896000531765
57	74140492	760224790	3411870849	54377527460	286536289525
58	97387056	678769206	7031029662	75712276810	784306233136
59	31312821	705257537	2515103006	22943051994	805459503577
60	82387746	552469185	7841126466	17939108714	723335325513
61	60986366	461477542	2530490810	57051442205	259302577763
62	75703401	953606850	2696117849	34820176671	572240858908
63	27464042	381084412	8417214051	44305877875	307359064348
64	56002467	949586749	6963861911	94751725183	801595835584
65	59620331	159524752	7168077974	85934247800	582397680149
66	24429582	231172352	9000141896	80404480320	453009746412
67	20640797	847231251	7959393264	29591740033	602558523846
68	61601423	915190201	3027039028	23778547388	123159642540
69	65885530	100096362	3275654012	93869421791	443196548673
70	18479921	116935512	9214457779	80234579742	198729629455
71	16862945	750771551	3161184684	80249967546	133109574076
72	63853750	764526952	7217327664	39914302785	420494988756
73	32920424	162176315	3595154464	57907948208	975851612875
74	31255973	571873640	7436198272	28875987033	559645047754
75	51898294	891350242	1147391738	20253357838	515410977136
76	78386625	605373287	2559873971	44048322494	330171922316
77	59816001	570051117	8213482157	67707685526	946351270862

Continued on next page

Table 5.28 – continued from previous page

Ref #	8 Digits	9 Digits	10 Digits	11 Digits	12 Digits
78	15243879	576381427	5488496564	69539749448	167168041201
79	58300482	338325266	3835191639	46386777396	672503985973
80	22648956	429516409	4220971953	20051167073	316743634717
81	54280381	162361065	1571213604	29455523196	198560622730
82	69524752	885646024	2214072539	21665563720	776680397324
83	86142611	456504794	8740009824	76595608988	810831734671
84	19883833	686314289	7989562509	89707157378	903731560158
85	10096362	110146328	1034763086	46520923052	442365266447
86	26935512	223154542	3293225236	20576246183	430390789287
87	57983973	512565683	7179026992	38117398376	108175679917
88	72176315	358368043	4274574484	50577066032	463510107747
89	79220456	821241591	5468789396	91518159752	969052139615
90	26214538	102025624	2086437636	44507130106	674081019884
91	77397933	411526687	7462942210	60920595976	639703917065
92	83728243	393054814	8828028661	83207973300	573607925886
93	94404206	356061060	6591305713	30015060823	695464058943
94	71080953	969610764	6359464643	81940448689	797628332934
95	72361065	881563360	3336703164	44930951972	597366716315
96	98069338	249125755	9107722004	61463846750	213095867233
97	59443377	282240337	6771746857	40474318427	837491010327
98	20146328	623149147	1142887412	17740009824	888789117562
99	19912499	406855912	1699530444	57577745160	152573214076
100	60152951	892862344	9063216615	61574370638	606458752129

Bibliography

[1] Robert G. Gallager, *Discrete Stochastic Processes*, Kluwer Academic Publishers, Norwell, Massachusetts, 3rd ed., 1996.

[2] Steven G. Krantz, *Real Analysis and Foundations*, Chapman & Hall, 2nd ed., 2004.

[3] J. C. Lagarias, *The 3x+1 Problem and its Generalizations*, the American Mathematics Monthly **92** (1985), no. 1, 3–23.

[4] G. Latouche, V. Ramaswami, *Introduction to Matrix Analytic Methods in Stochastic Modelling*, PH Distributions, ASA SIAM, 1st ed., 1999.

[5] Toms Oliveira e Silva, (January 19, 2009). *3x+1 conjecture verification results*. Retrieved July 14, 2009 from http://www.ieeta.pt/ tos/3x+1.html.