CYCLES OF DIRECTED GRAPHS DEFINED BY MATRIX MULTIPLICATION (MOD n)

Ezra Brown

Virginia Tech

Blacksburg VA 24061–0123

brown@math.vt.edu

Theresa P. Vaughan

University of North Carolina at Greensboro

Greensboro NC 27402–6170

tpvaugha@euler.uncg.edu

CYCLES OF DIRECTED GRAPHS DEFINED BY MATRIX MULTIPLICATION (MOD n)

EZRA BROWN AND THERESA VAUGHAN

Key Words: Digraph cycle, cycle length, characteristic polynomial, minimal polynomial, Smith form

Abstract: Let A be a $k \times k$ matrix over a ring R; let $GM(A, R)$ be the digraph with vertex set R^k, and an arc from v to w if and only if $w = Av$. In this paper, we determine the numbers and lengths of the cycles of $GM(A, R)$ for $k = 2$ in the following two cases. (a) $R = \mathbb{F}_q$, the q–element finite field, and (b) $R = \mathbb{Z}/n\mathbb{Z}$ and $\mathrm{GCD}(n, det(A)) = 1$. This extends previous results for $k = 1$ and $R = \mathbb{Z}/n\mathbb{Z}$. We make considerable use of the Smith form of a matrix; other than that, the most powerful tool we use is the Chinese Remainder Theorem.

1. Introduction

For a an integer and n a positive integer, let $G(a, n)$ (respectively, $GP(a, n)$) be the digraph with vertex set $\{0, 1, \ldots, n-1\} = \mathbb{Z}/n\mathbb{Z}$ such that there is an arc from x to y if and only if $y \equiv ax \pmod{n}$ (respectively, $y \equiv x^a \pmod{n}$). Unlike many iterative processes, linearity here leads to a high degree of symmetry in the underlying graph. Previously (see [1]) we determined the number of cycles in $G(a, n)$ for n a positive integer, and in $GP(a, n)$ for the case that n is a prime power. This notion can be generalized in the following way. Let A be a $k \times k$ matrix with coefficients in a ring R; let $GM(A, R)$ be the digraph with vertex set R^k such that there is an arc from v to w if and only if $w = Av$. We will also write $GM(A, n)$ to mean the digraph $GM(A, \mathbb{Z}/n\mathbb{Z})$.

A few small examples are sufficient to exhibit the structure of these graphs. Suppose R is either $\mathbb{Z}/n\mathbb{Z}$ or a finite field. If A is nonsingular then $GM(A, R)$ is a collection of disjoint directed cycles; if A is singular then $GM(A, R)$ is a collection of disjoint directed cycles with pendant trees. Among the salient features of these

Date: February 13, 2003.

graphs are the numbers and lengths of the disjoint cycles, which we study in this paper. In particular, we study the cycle structure of these digraphs $GM(A, R)$ for 2×2 matrices, limiting the scope of our investigation to these cases: (a) $R = \mathbb{F}_q$, the q–element finite field, and (b) $R = \mathbb{Z}/n\mathbb{Z}$ and $\mathrm{GCD}(n, det(A)) = 1$.

For case (a), we are able to treat all matrices, using the result that similar matrices induce isomorphic digraphs. For case (b), it suffices to consider n a prime power by means of an argument using the Chinese Remainder Theorem; we also make considerable use of the Smith form of a matrix. In Section 2, we prove a theorem which allows us to simplify our work by making appropriate assumptions about our matrices. In Section 3 we prove a structure theorem for all 2×2 matrices over arbitrary finite fields. Section 4 is devoted to the development of results about the Smith form, which we will use later. In Section 5 we study the structure of $GM(A, p^j)$ for A nonsingular mod p, obtaining results about the order of A modulo arbitrary powers of p; this study breaks naturally into two cases: p odd and $p = 2$. In Section 6, we state some of the results which allow us to count the numbers and lengths of the cycles of $GM(A, q)$ for prime powers q; as these results are quite complicated, not all of the results (as well as their proofs) are included, but are available from the authors on request.

2. Digraphs defined by linear transformations

Let V be a vector space over the finite field F and let T be a linear transformation of V to itself (i.e. a linear operator on V). Let $GM(T, F)$ be the digraph with vertex set V such that (v, w) is an arc if and only if $w = T(v)$. A cycle in $GM(T, F)$ must necessarily be a directed cycle — otherwise, there are arcs (v, w) and (v, x) with $w \neq x$, which is impossible, since T is well–defined. Hence, a cycle is of the form

$$C = (v, T(v), T^2(v), ..., T^{r-1}(v)) \tag{2.1}$$

where $T^r(v) = v$ and r is the least such positive integer. The study of cycles in $GM(T, F)$, then, involves the study of vectors of finite period under T.

We are mainly interested in the case in which both F and $\dim(V)$ are finite, but the general theory is also of interest. Our first observation, an easy consequence of the definitions, is that similar linear transformations generate isomorphic digraphs.

Lemma 2.1. *Let V be a vector space over the field F. If T and Q are linear operators on V and Q is invertible, then the map*

$$Q : GM(T, F) \to GM(QTQ^{-1}, F), \tag{2.2}$$

which maps v to $Q(v)$, is a digraph isomorphism.

Now let A be a $k \times k$ matrix over the finite field $\mathbb{F}_q$ of order $q = p^n$ (p a prime). The map $L_A : V \to V$ defined by $L_A(v) = Av$ is a linear operator, and we write $GM(A,\ \mathbb{F}_q)$ (instead of $GM(L_A,\ \mathbb{F}_q)$) for the relevant digraph. For such graphs, the following useful corollary is an immediate consequence of Theorem 2.1.

Corollary 2.2. *If A and B are similar matrices over $\mathbb{F}_q$, then the digraphs $GM(A,\ \mathbb{F}_q)$ and $GM(B,\ \mathbb{F}_q)$ are isomorphic.*

3. The structure of $GM(A,\ \mathbb{F}_q)$ for 2×2 matrices

If $\alpha \neq 0$ lies in a finite extension of $\mathbb{F}_q$, we define the *order* $ord_q(\alpha)$ of α to be the least positive integer r for which $\alpha^r = 1$. This work began as an effort to extend the results of [1], which describes the cycle structure of $G(a, n)$ the digraph on $\{0, 1, \ldots, n-1\}$ such that (x, y) is an arc if and only if $y \equiv zx \pmod{n}$. If we replace modular multiplication of numbers by multiplication of a vector by a 2×2 matrix, all over a finite field $\mathbb{F}_q$, then we have the following structure theorem.

Theorem 3.1. *Let $q = p^n$ be a prime power, let $\mathbb{F}_q$ be the finite field with q elements, let A be a 2×2 matrix over $\mathbb{F}_q$, and let λ and μ be the roots of the characteristic polynomial of A. Then the number of cycles in $GM(A,\ \mathbb{F}_q)$ is given by the following table:*

Case	*Conditions on λ, μ*	*Number of cycles in $GM(A,\ \mathbb{F}_q)$*
I.	*λ, μ distinct and nonzero*	
I(a)	$\lambda, \mu \in \mathbb{F}_q$	$1 + \frac{q-1}{ord_q(\lambda)} + \frac{q-1}{ord_q(\mu)} + \frac{(q-1)^2}{LCM[ord_q(\lambda), ord_q(\mu)]}$
I(b)	$\lambda, \mu \notin \mathbb{F}_q$	$1 + \frac{q^2-1}{ord_q(\lambda)}$
II	$\lambda \neq 0, \mu = 0$	$1 + \frac{q-1}{ord_q(\lambda)}$
III.	$\lambda = \mu \neq 0$, *one–dim. eigenspace*	$1 + \frac{q-1}{ord_q(\lambda)} + \frac{q(q-1)}{p \cdot ord_q(\lambda)}$
IV.	$\lambda = \mu \neq 0$, *two–dim. eigenspace*	$1 + \frac{q^2-1}{ord_q(\lambda)}$
V.	$\lambda = \mu = 0$	1

Proof. Let $V = \mathbb{F}_q^2$ be the 2–dimensional vector space over $\mathbb{F}_q$. We note that v is on a cycle of $GM(A, \mathbb{F}_q)$ if and only if $A^r v = v$ for some positive integer r. If $S \subseteq V$, let $< S >$ denote the subgraph of $GM(A, \mathbb{F}_q)$ induced by S.

Case I(a): $\lambda, \mu \in \mathbb{F}_q$, distinct, nonzero. Let e_λ and e_μ be eigenvectors associated with λ and μ respectively. Since $\lambda, \mu \in \mathbb{F}_q$, it follows that $\{e_\lambda, e_\mu\}$ is a basis for V, so that we may write each $v \in V$ uniquely as $v = v_\lambda e_\lambda + v_\mu e_\mu$ with $v_\lambda, v_\mu \in \mathbb{F}_q$. It follows that

$$Av = v_\lambda \lambda e_\lambda + v_\mu \mu e_\mu, \text{ and in general,} \tag{3.1}$$

$$A^r v = v_\lambda \lambda^r e_\lambda + v_\mu \mu^r e_\mu, \tag{3.2}$$

for r a positive integer. Since λ and μ are nonzero, we have that

$$A^r v = v \text{ if and only if } \begin{cases} \lambda^r = \mu^r = 1 & (v_\lambda \neq 0 \neq v_\mu); \\ \lambda^r = 1 & (v_\lambda \neq 0, v_\mu = 0); \\ \mu^r = 1 & (v_\lambda = 0, v_\mu \neq 0. \end{cases} \tag{3.3}$$

Hence the cycle containing v has length

$$LCM[ord_q(\lambda), ord_q(\mu)], \quad \text{if} \quad v_\lambda \neq 0 \neq v_\mu; \tag{3.4}$$

$$ord_q(\lambda), \quad \text{if} \quad v_\lambda \neq 0, v_\mu = 0; \tag{3.5}$$

$$ord_q(\mu), \quad \text{if} \quad v_\lambda = 0, v_\mu \neq 0. \tag{3.6}$$

Now there are $(q-1)^2$ vectors $v = v_\lambda e_\lambda + v_\mu e_\mu$ with both v_λ and v_μ nonzero elements of $\mathbb{F}_q$, $q-1$ with $v_\lambda = 0$ and v_μ a nonzero element of $\mathbb{F}_q$, and $q-1$ with v_λ a nonzero element of $\mathbb{F}_q$ and $v_\mu = 0$. Since the above argument about cycle length is independent of choice of v, we have that $< \{v : v_\lambda \neq 0 \neq v_\mu\} >$ contains $\dfrac{(q-1)^2}{LCM[ord_q(\lambda), ord_q(\mu)]}$ cycles, $< \{v : v_\lambda \neq 0, v_\mu = 0\} >$ contains $\dfrac{q-1}{ord_q(\lambda)}$ cycles, and $< \{v : v_\lambda = 0, v_\mu \neq 0\} >$ contains $\dfrac{q-1}{ord_q(\mu)}$ cycles. This leaves only the zero vector, which lies on a cycle by itself, and establishes I(a).

Case I(b): λ, μ distinct and not in $\mathbb{F}_q$. The analysis of Case I(a) applies, with the following exception. If $v \in V$ and $\lambda \notin \mathbb{F}_q$, then $Av \in V$, but $\lambda \notin \mathbb{F}_q$; hence, no vector in V is an eigenvector of A. It follows that the eigenspaces of A intersect V only in the zero vector. Now even though $\lambda, \mu \notin \mathbb{F}_q$, they both lie in a quadratic extension of $\mathbb{F}_q$, so that $ord_q(\lambda)$ and $ord_q(\mu)$ are both defined. Furthermore, λ and μ are conjugate over $\mathbb{F}_q$ so that they have the same order over $\mathbb{F}_q$. Thus, each of the $q^2 - 1$ nonzero vectors in V is on a cycle of length $ord_q(\lambda)$;

together with the zero vector (a cycle on its own), this yields a total of $1 + \dfrac{q^2-1}{ord_q(\lambda)}$ cycles in all.

Case II: $\lambda \neq 0, \mu = 0$. As before, let $v = v_\lambda e_\lambda + v_0 e_0$ be a nonzero vector. Then $Av = v_\lambda Ae_\lambda + v_0 Ae_0 = v_\lambda \lambda e_\lambda$ (since $\mu = 0$), and so $A^r v = v_\lambda \lambda^r e_\lambda$. Hence, v lies on a cycle if and only if $\lambda^r e_\lambda = v_\lambda e_\lambda + v_0 e_0$ for some $r \geq 1$. It follows that the only vectors on cycles are those for which $v_0 = 0$, i.e. multiples of the eigenvector e_λ. There are clearly $q-1$ such nonzero vectors, and as before, each one is on a cycle of length $ord_q(\lambda)$. Together with the zero vector, this yields $1 + \dfrac{q-1}{ord_q(\lambda)}$ cycles in all.

Case III: $\lambda = \mu$, one–dimensional eigenspace. In this case, A is similar to a matrix of the form

$$B = \begin{pmatrix} \lambda & b \\ 0 & \lambda \end{pmatrix} \tag{3.7}$$

with $b \neq 0$. By Theorem 1, the cycle structures $GM(A,\ \mathbb{F}_q)$ and $GM(B,\ \mathbb{F}_q)$ are the same, so we may work with $GM(B,\ \mathbb{F}_q)$ instead. We see that

$$B^r = \begin{pmatrix} \lambda^r & r\lambda^{r-1}b \\ 0 & \lambda^r \end{pmatrix}; \tag{3.8}$$

let us write $v = (v_1, v_2)$. If $v_2 = 0$, then $Bv = (\lambda v_1, 0) = \lambda v$. In this case, it is clear that the cycle length is equal to 1 or $ord_q(\lambda)$ according as $v_1 = 0$ or $v_1 \neq 0$, so that $< v : v_2 = 0 >$ contains $1 + \dfrac{q-1}{ord_q(\lambda)}$ cycles.

If $v_2 \neq 0$, then $B^r v = (\lambda^r v_1 + r\lambda^{r-1} b v_2, \lambda^r v_2)$, so that $B^r v = v$ if and only if $r = 0$ in the field $\mathbb{F}_q$, since $\lambda \neq 0 \neq b$, and $\lambda^r = 1$. This occurs if and only if $ord_q(\lambda) | (q-1)$ and $p | r$, where $q = p^n$ and p is a prime. Since $ord_q(\lambda) | (q-1)$, we know that p and $ord_q(\lambda)$ are relatively prime. Thus, if $v_2 \neq 0$, then v lies on a cycle of length $p \cdot ord_q(\lambda)$. Since there are $q^2 - q$ vectors with $v_2 \neq 0$, we see that $< v : v_2 \neq 0 >$ contains $\dfrac{q(q-1)}{p \cdot ord_q(\lambda)}$ cycles.

We conclude that if A has a single eigenvalue of multiplicity 2 and a one–dimensional eigenspace, then $GM(A,\ \mathbb{F}_q)$ contains

$$1 + \frac{q-1}{ord_q(\lambda)} + \frac{q(q-1)}{p \cdot ord_q(\lambda)} \tag{3.9}$$

cycles in all.

Case IV: $\lambda = \mu \neq 0$, two–dimensional eigenspace. Such a matrix A is similar to $B = \lambda I$ with $\lambda \neq 0$. Hence, for all v, $B^r v = v$ if and only if either (1)

$v = 0$ or (2) $v \neq 0$ and $\lambda^r v = v$, i.e. $ord_q(\lambda)|r$. It follows that every nonzero vector — and there are $q^2 - 1$ of them — is in a cycle of length $ord_q(\lambda)$, and there is also the zero cycle. Hence, $GM(A,\ \mathbb{F}_q)$ contains $1 + \dfrac{q^2-1}{ord_q(\lambda)}$ cycles in all.

Case V: $\lambda = \mu = 0$. In this case, the only vector that lies on a cycle is the zero vector, as A is similar to a matrix of the form $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$. Hence, $GM(A,\ \mathbb{F}_q)$ contains just one cycle. □

4. The Smith form of a matrix, and reduction to prime powers

Let $\mathrm{diag}(a, b)$ denote the matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$; let X be an integral 2×2 matrix. Then there exist unimodular integral 2×2 matrices P and Q such that $PXQ = D = \mathrm{diag}(d_1, d_2)$ where d_1, d_2 are non-negative integers, d_1 divides d_2, $d_1 d_2 = |det(X)|$, and d_1 is the greatest common divisor of the entries of X. The matrix D is called the Smith form of the matrix X. For a detailed discussion, see [4].

The Smith form of the matrix $A^j - I$ can be used to give information about the number and nature of solutions to the matrix congruence $A^j v \equiv v \bmod n$, where n is an integer. We first establish some notation, to be used throughout this section; in what follows X, P, Q are defined as above, and we let $\mathrm{col}(x, y)$ denote the column vector $\begin{pmatrix} x \\ y \end{pmatrix}$.

We will make use of the following key point throughout the paper:

Let C_1, C_2 be the columns of Q, and E_1, E_2 the columns of P^{-1}. Let $\mathrm{col}(x, y) \in \mathbf{Z}_n^2$. Then $v = \mathrm{col}(x, y) = Q{\cdot}\mathrm{col}(r, s)$ for some $r, s \in \mathbf{Z}$, and putting $\mathrm{col}(r, s) = u$, we have $Xv = XQu = P^{-1}Du = d_1 r E_1 + d_2 s E_2$. Since P^{-1} is unimodular, it is invertible mod n for every positive integer n. In particular, its columns E_1, E_2 are "independent" mod n, i.e. if a, b are integers, then $aE_1 + bE_2 \equiv 0 \bmod n$ if and only if $a \equiv b \equiv 0 \bmod n$.

Lemma 4.1. *Let $n = p^t$. Then the matrix equation $Xv \equiv 0$ mod n has a solution v such that $v \not\equiv 0$ mod p, if and only if n divides d_2.*

Proof. Suppose first that n divides d_2. Choose $r = 0$ and $s = 1$, and put $\mathrm{col}(r, s) = u$. Then $\mathrm{col}(x, y) = Qu \not\equiv 0 \bmod p$, since Q is unimodular and $u \not\equiv 0 \bmod p$, and $Xv = XQu = d_1 r E_1 + d_2 s E_2 = d_2 E_2 \equiv 0 \bmod n$.

On the other hand, suppose that $Xv \equiv 0 \bmod n$ has a solution v such that $v \not\equiv 0 \bmod p$. Then $Xv = XQu = d_1 r E_1 + d_2 s E_2$ where $v = Qu$ with $\mathrm{col}(r, s) = u$, and $u \not\equiv 0 \bmod p$ (again, since Q is unimodular and $v \not\equiv 0 \bmod p$). Then $n = p^t$ must divide $d_1 r$ and $d_2 s$. Since $u \not\equiv 0 \bmod p$, then either r or s must be relatively prime to p, and hence p^t must divide either d_1 or d_2. But d_1 divides d_2, so in either case, p^t divides d_2. □

The equation $Xv = d_1 r E_1 + d_2 s E_2$ then allows a count of the number of solutions mod n.

Theorem 4.2. *Let $n = p^t$. Let N be the number of solutions v of the matrix equation $Xv \equiv 0$ mod n, such that $v \not\equiv 0$ mod p. Suppose that $N > 0$. If p^t divides d_1, then $N = p^{2t} - p^{2t-2}$, and if $d_1 = p^i m$ where m is relatively prime to p and $0 \leq i < t$, then $N = p^i \phi(p^t)$.*

Proof. Since $N > 0$, then by Lemma 4.1, d_2 is a multiple of p^t. Write $d_1 = p^i m$, where either $m = 0$ or p does not divide m.

If $m = 0$, or if $i \geq t$, then every vector v mod n is a solution of $Xv \equiv 0$ mod n. Then N is the number of vectors v mod p^t such that $v \not\equiv 0$ mod p and $N = p^{2t} - p^{2t-2}$.

Suppose $m \neq 0$ and $0 \leq i < t$. Write $v = \mathrm{col}(x, y) = Q \cdot \mathrm{col}(r, s)$ where $r, s \in \mathbf{Z}$, and put $\mathrm{col}(r, s) = u$. Suppose that v is a solution of $Xv \equiv 0 \bmod p^t$, with $v \not\equiv 0$ mod p. Then $Xv = XQu = d_1 r E_1 + d_2 s E_2 \equiv 0 \bmod p^t$, and then p^{t-i} must divide r. In order for $v \not\equiv 0$ mod p it is necessary and sufficient that $u \not\equiv 0$ mod p (since Q is unimodular). Since p^{t-i} divides r, s must be relatively prime to p.

The number of integers r mod p^t which are multiples of p^{t-i}, is just p^i, and the number of integers s mod p^t which are relatively prime to p, is $\phi(p^t)$. Thus the number of such vectors $\mathrm{col}(r, s) \equiv u$ mod p^t is $N = p^i \phi(p^t)$. □

The final result in this section reduces the study of the structure of $GM(A, n)$ to that of $GM(A, p^r)$, where p is a prime.

Theorem 4.3. *Let $S(A, k, n)$ be the number of vectors $w \in (\mathbb{Z}/n\mathbb{Z})^2$ for which $A^k w \equiv w \pmod n$. If $GCD(m, n) = 1$, then $S(A, k, mn) = S(A, k, m) \cdot S(A, k, n)$.*

Proof. Let $w = \mathrm{col}(x, y)$. Since $\mathrm{GCD}(m, n) = 1$, there exist integers x_1, x_2, y_1 and y_2 such that

$$u = mx_1 + nx_2 \qquad \text{and} \qquad v = my_1 + ny_2.$$

If k is a nonnegative integer, then

$$A^k \begin{pmatrix} u \\ v \end{pmatrix} = m \cdot A^k \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + n \cdot A^k \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Thus, $A^k w \equiv w \pmod{mn}$ if and only if

$$(A^k - I) \begin{pmatrix} u \\ v \end{pmatrix} = m \cdot (A^k - I) \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + n \cdot (A^k - I) \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \equiv 0 \pmod{mn}.$$

But since m and n are relatively prime, the Chinese Remainder Theorem implies that this is true if and only if

$$(A^k - I) \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \equiv 0 \pmod{n} \qquad \text{and} \qquad (A^k - I) \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \equiv 0 \pmod{m}$$

are true. It follows that $S(A, k, mn) = S(A, k, m) \cdot S(A, k, n)$. □

At this point, we should note that in all of our subsequent results concerning the order of A mod p^n, we are assuming that if $A^k \equiv I \bmod p^n$, then A^k is not, in fact, equal to the identity matrix I.

For suppose that A is a 2×2 integer matrix and $A^k = I$ for some positive integer k. Then (see [2]) the minimum polynomial for A has degree 1 or 2, and also divides $x^k - 1$; thus the eigenvalues of A are roots of unity, with algebraic degree either 1 or 2. Since (see [3]) a primitive $m-$th root of unity has algebraic degree $\phi(m)$, then the eigenvalues of A can only be $m-$th roots of unity for $m = 1, 2, 3, 4, 6$. Then A can have the following possible minimal polynomials, characteristic polynomials and cycle lengths:

Minimal Polynomial	Characteristic Polynomial	Possible Cycle Lengths
$x - 1$	$(x-1)^2$	1 (A =diag$(1, 1)$)
$x + 1$	$(x+1)^2$	2 (A =diag$(-1, -1)$)
$x^2 - 1$	$x^2 - 1$	1, 2
$x^2 + 1$	$x^2 + 1$	1, 2, 4
$x^2 + x + 1$	$x^2 + x + 1$	1, 3
$x^2 - x + 1$	$x^2 - x + 1$	1, 3, 6

5. The Order of A mod p^j

By Theorem 4.3, we need only study the structure of $GM(A, q)$ for prime powers q, so let p be a fixed prime and let A be an integral 2×2 matrix. We are assuming that A is non–singular mod p^j, that is, $\det(A)$ is not divisible by p. Then A is a member of the (finite) group of non–singular 2×2 matrices mod p^j, and so it has finite order in that group. From now on, we assume that A does not have finite order in $GL(2, \mathbb{Z})$, i.e. $A^k \neq I$ for any positive integer k.

Definition 5.1. *Let k_j denote the order of A mod p^j, i.e. k_j is the least positive integer t such that $A^t \equiv I$ mod p^j.*

Since $A^{k_1} \equiv I \bmod p$ and $A^{k_1} \neq I$, it follows that $A^{k_1} = I + p^s B$ where B is an integral 2×2 matrix, such that $s > 0$ and $B \not\equiv 0 \bmod p$. We will use the letters B and s throughout in this sense.

Lemma 5.2. *For all $j = 1, 2, \cdots$, we have $k_j | k_{j+1}$.*

Proof. Put $m = k_{j+1}$. Since $A^m \equiv I \bmod p^{j+1}$, then it is also true that $A^m \equiv I \bmod p^j$. Then the order of A mod p^j must divide m, as required. □

The next two theorems show that the quotient k_{j+1}/k_1 is always a power of p, described in terms of the integer s defined above. We use the notation $C(n, k)$ for the binomial coefficient "n choose k".

Theorem 5.3. *If p is odd, or if $s > 1$, then $k_1 = k_2 = \cdots = k_s$ and for all $i = 1, 2, \cdots$, $k_{s+i} = p^i k_1$.*

Proof. Suppose that either p is odd, or $p = 2$ and $s > 1$. We have $A^{k_1} = I + p^s B$, and clearly for every p^j with $j \leq s$, we have $A^{k_1} \equiv I \bmod p^j$. Thus for these values of j, it follows that $k_j | k_1$. By Lemma 5.2, we also have $k_1 | k_j$ and so $k_j = k_1$ for all $j = 1, 2, \cdots s$. □

Next, we consider the case $j = s + 1$. By the Binomial Theorem, we know that

$$A^{pk_1} = I + C(p, 1)p^s B + C(p, 2)p^{2s} B^2 + \cdots + p^{ps} B^p.$$

Since $s \geq 1$, the term $p^{ps} B^p$ is a multiple of p^{s+1}. If p is odd, then all the coefficients $C(p, i)$ with $1 \leq i < p$ are multiples of p, and so all terms $C(p, i)p^{is} B^i$ are also

multiples of p^{s+1}. If $s > 1$, then for $i = 2, 3, \cdots$, we have $is > s + 1$, and (since $C(p, 1) = p$) again all terms with $i > 0$ are multiples of p^{s+1}.

It follows that $A^{pk_1} \equiv I \bmod p^{s+1}$, and so $k_{s+1}|pk_s$ (since $k_s = k_1$). Since $B \not\equiv 0 \bmod p$, then $A^{k_1} \not\equiv I \bmod p^{s+1}$, that is, $k_{s+1} \neq k_s$. It follows that $k_{s+1} = pk_s$.

Now note that for $i > 1$, the i^{th} term above is actually a multiple of p^{s+2}, and so we have

$$A^{k_{s+1}} = I + p^{s+1}B_1,$$

where $B_1 \equiv B \bmod p$. Applying the same argument to this matrix equation, we find that $k_{s+2} = pk_{s+1}$ and $A^{k_{s+2}} = I + p^{s+2}B_2$ where $B_2 \equiv B \bmod p$, and the statement of the theorem follows by induction.

The case when $p = 2$ and $s = 1$ is a little different, since $s + 1 = 2s$.

Theorem 5.4. *Suppose that $p = 2$ and $s = 1$. Then one of the following must occur:*

(i) $k_i = 2^{i-1}k_1$ for all $i = 2, 3, \cdots$.

(ii) There exists an integer $t \geq 2$ such that $k_i = 2k_1$ for $2 \leq i \leq t$, and $k_i = 2^{i-t}k_2$ for all $i > t$.

Proof. We begin with the matrix equation $A^{k_1} = I + 2B$, where $B \not\equiv 0 \bmod 2$. Then

$$A^{2k_1} = I + 4B + 4B^2 = I + 4C,$$

where it is possible that the matrix C satisfies $C \equiv 0 \bmod 2$. However, since we are assuming that the matrix $A^i \neq I$ for any integer i, we can say that $C \neq 0$.

If $C \not\equiv 0 \bmod 2$, then (i) follows, by the argument used in the proof of Theorem 5.3.

On the other hand, if $4C = 2^tC_1$, where $C_1 \not\equiv 0 \bmod 2$, then (again, as in Theorem 5.3) we find that $k_j = k_2$ for all $j = 2, 3, \cdots t$ and for all $i = 1, 2, \cdots$, $k_{t+i} = 2^ik_2$, which is (ii). □

6. Counting cycles of A (mod p^j)

Throughout this section, let the prime p and the positive integer j be fixed, and put $n = p^j$. We also assume that there is no positive integer m such that $A^m = I$.

Recall that Theorem 3.1, which gives the structure of $GM(A, \mathbb{F}_q)$ for matrices over finite fields, is fairly straightforward. When we replace finite fields with the

rings $\mathbb{Z}/p^n\mathbb{Z}$, the treatment divides into four cases, according to the nature of characteristic and minimum polynomials for A mod p. We shall treat Case (i) in its entirety. The other three cases produce an elaborate set of subcases, and the results are straightforward but quite complicated. Hence, we will state a few representative results from these cases; complete treatments of Cases (ii), (iii) and (iv) are available from the authors.

Definition 6.1. *Let p be a fixed prime, j an integer. Divide the set $(\mathbb{Z}/p^j\mathbb{Z})^2$ into disjoint subsets X_i, for $0 \leq i \leq j$, as follows: $X_j = \{col(0,0)\}$, and if $i < j$, then $X_i = \{col(p^i x, p^i y) | x \text{ or } y \not\equiv 0 \text{ mod } p \text{ and } 0 \leq x, y < p^{j-i}\}$.*

For example, $X_2(3^3) = \{(0,9),(0,18),(9,0),(9,9),(9,18),(18,9),(18,18)\}$. We abuse the notation by just saying X_0, e.g., instead of $X_0(p^j)$. Note that the cardinality of the set X_i, for $0 \leq i < j$, is given by $|X_i| = p^{2(j-i)} - p^{2(j-i-1)}$

As noted also in Section 4, since A is non-singular mod p^j, $v \in X_i$ if and only if $Av \in X_i$; and if $v \in X_i$, $v = p^i \cdot \text{col}(x,y) = p^i w$, then $A^m v \equiv v \text{ mod } p^j$ if and only if $A^m w \equiv w \text{ mod } p^{j-i}$. Thus it suffices to find the cycle structure in the set X_0, mod p^j, for each $j = 1, 2, \cdots$.

Now let $N(m, p^j)$ denote the number of cycles of A, of length m, in the set X_0, and let $M(k, p^j)$ be the number of vectors $v \in X_0$ mod p^j such that $A^k v \equiv v$ mod p^j. These two quantities are related by the following result.

Lemma 6.2. *Suppose that A is nonsingular mod p, and $j > 0$. Let $L_1 < L_2 < \cdots < L_m$ be the lengths of the cycles $(\text{mod } p^j)$ in X_0 $(\text{mod } p^j)$. If $L_i | L_{i+1}$ for $i = 1, \ldots, m-1$ then:*

$$N(L_i, p^j) = \begin{cases} M(L_1, p^j)/L_1, & \text{if } i = 1; \\ (M(L_i, p^j) - M(L_{i-1}, p^j))/L_i, & \text{if } 1 < i < m; \\ (X_0 - M(L_{m-1}, p^j))/L_M, & \text{if } i = m. \end{cases}$$

Proof. Let $1 \leq i \leq m$. By definition, $M(L_i, p^j)$ is the set of solutions v $(\text{mod } p^j)$ of $(A^{L_i} - I)v \equiv 0 \ (\text{mod } p^j)$. If $k < i$, then $x^{L_k} - 1$ divides $x^{L_i} - 1$, and so every solution of $(A^{L_k} - I)v \equiv 0 \ (\text{mod } p^j)$ is also a solution of $(A^{L_i} - I)v \equiv 0 \ (\text{mod } p^j)$. Hence if $k < i$, then $M(L_i, p^j) - M(L_{i-1}, p^j)$ counts the number of vectors v whose cycle length is L_i if $i > 1$, and $M(L_1, p^j)$ counts the number of vectors v whose cycle length is L_1. The lemma follows. □

We compute the quantities $N(m, p^j)$ in four separate cases, according to the nature of the characteristic and minimum polynomials for A mod p (f and g, respectively):

CASE (i) $f(x) = g(x)$ is irreducible mod p

CASE (ii) $f(x) = (x-a)(x-b)$ mod p, with $a \not\equiv b$ mod p

CASE (iii) $f(x) = (x-a)^2$, and $g(x) = x - a$ mod p

CASE (iv) $f(x) = g(x) = (x-a)^2$ mod p

Since the finite field $GF(p)$ is indeed a field, we have the following well-known results of linear algebra. Let $h(x)$ be any polynomial with integral coefficients. Then:

(a) $h(A) \equiv 0$ mod p if and only if $g(x)$ divides $h(x)$ mod p,

(b) If $v \not\equiv 0$ mod p, and if $h(A)v \equiv 0$ mod p, then $\gcd(f(x), h(x)) \neq 1$ mod p.

CASE (i) $f(x) = g(x)$ **is irreducible mod** p**.**

We will treat this case in its entirety. We first summarize some well–known properties of such a polynomial mod p.

The polynomial $f(x)$ factors in the finite field $GF(p^2)$; its roots are distinct and have the same order, say m, in the multiplicative group of the field. Then the polynomial $f(x)$ divides $x^m - 1$ mod p, and $f(x)$ does not divide $x^k - 1$ mod p for any k less than m. Then $A^m \equiv I$ mod p, and if k is less than m, $A^k \not\equiv I$; that is m is the order of the matrix A in the group of non-singular 2×2 matrices mod p, or, in the notation of Section 5, we have $k_1 = m$.

Theorem 6.3. *Let $n = p^t$ and suppose that $f(x)$ is irreducible mod p. Then all cycles of A in the set X_0 have the same length k_t, and $N(k_t, p^t) = |X_0|/k_t = (p^{2(t)} - p^{2(t-1)})/k_t$.*

Proof. Put $m = k_1$. By the Division Algorithm, we have

$$x^m - 1 = g(x)q(x) + p^s r(x),$$

where $s \geq 1$ and $r(x)$ is a polynomial of degree 0 or 1 which is not 0 mod p. (Note that $r(x)$ cannot be 0 since we always assume that $A^j \neq I$ for any positive integer j.) Then

$$A^m - I = g(A)q(A) + p^s r(A) = p^s r(A) = p^s B.$$

It follows from Section 5 that we have $k_1 = \cdots = k_s$, $k_{s+i} = p^i k_1$, and if $j = k_{s+i}$ with $i > 0$, $A^j - I \equiv p^{s+i}B \bmod p^{s+i+1}$.

Since $B = r(A)$ is a polynomial in A and $\gcd(f(x), r(x)) = 1$, then B is non-singular mod p, i.e. $\det(B) \neq 0 \bmod p$, and the Smith form $S(B)$ of B is of the form $S(B) = \mathrm{diag}(a, b)$, where $a, b \not\equiv 0 \bmod p$.

Then $S(A^m - I) = \mathrm{diag}(p^s a, p^s b)$, and if $j = k_{s+i}$ with $i > 0$, $S(A^j - I) \equiv \mathrm{diag}$ $(p^{s+i}a, p^{s+j}b) \bmod p^{s+i+1}$.

Clearly, for any integer t and vector $v \not\equiv 0 \bmod p$, $(A^j - I)v \equiv 0 \bmod p^t$ if and only if $(A^j - I) \equiv 0 \bmod p^t$, and so every vector $v \in X_0 \bmod p^t$ has the same cycle length, namely k_t. Since the cycles partition X_0, the result follows. □

CASE (ii) $f(x) = (x - a)(x - b)$ **mod** p**, with** $a \not\equiv b$ **mod** p**.**

Theorem 6.4. *(One of nine subcases in all.) Let p be an odd prime. Suppose that $A = D_j + p^j B_j$ where D_j and B_j are integral matrices, and $D_j = diag(a_j, b_j)$. Let m_j, n_j denote the orders of a_j, b_j mod p^j respectively, and define r_j, s_j by $m_j = p^{r_j} m_1$ and $n_j = p^{s_j} n_1$; without loss of generality, assume that $r_j \geq s_j$. Let k_j be the order of A mod p^j and let k be the least common multiple of m_1 and n_1. Write $A^{k_1} = I + p^t C$, with $C \not\equiv 0 \pmod p$ and $t \geq 1$.*

If $r_j > s_j$ and m_1 and n_1 do not divide each other, then the distinct cycle lengths in $X_0 \pmod{p^j}$ are $p^{s_j} n_1, p^{r_j} m_1$ and $p^{r_j - t} k$ for $0 \leq t \leq r_j - s_j$, and their numbers are as follows:

$$N(p_j^s n_1, p^j) = \varphi(p^{j-s_j})/n_1,$$
$$N(p^{r_j} m_1, p^j) = \varphi(p^{j-r_j})/m_1,$$
$$N(p^{r_j} k, p^j) = (p^j - 1)\varphi(p^{j-r_j})/k,$$
$$N(p^{s_j} k, p^j) = (p^u - 1)\varphi(p^{j-s_j})/k, \text{ and}$$
$$N(p^{r_j - t} k, p^j) = \varphi(p^u)\varphi(p^{j-s_j})/k \text{ (for } 0 < t < r_j - s_j),$$

where u is defined as follows: for $c = p^{s_j} k$, put $a_j^c = 1 + p^u \alpha$ with $p \nmid \alpha$ and $1 \leq u < j$.

CASE (iii) $f(x) = (x - a)^2$**, and** $g(x) = x - a$ **mod** p

Theorem 6.5. *(Three of sixteen subcases.) Suppose that $A^{k_1} = I + p^s B$ where $s \geq 1$, and B is singular mod p, $B \not\equiv 0$ mod p, and write $det(B) = p^t b$, where $t \geq 1$*

and b is relatively prime to p. Suppose also that either p is odd, or $p = 2$ and $s > 1$. Then:

(i) If $1 \le j \le s$, then $N(k_1, p^j) = |X_0|/k_1$.

(ii) If $j = s + r$ with $1 \le r \le t$, so that the cycle lengths are $k_1, pk_1, \ldots, p^r k_1$, then

$$N(k_1, p^j) = N(p^r k_1, p^j) = p^s \varphi(p^j)/k_1,$$

and for $1 < i < r$,

$$N(p^i k_1, p^j) = \varphi(p^s)\varphi(p^j)/k_1.$$

(iii) If $j = s+t+k$ with $k \ge 1$, so that the cycle lengths are $p^k k_1, p^{k+1} k_1, \ldots, p^{k+t} k_1$, then

$$N(p^k k_1, p^j) = N(p^{k+t} k_1, p^j) = p^s \varphi(p^j)/k_1,$$

and for $1 < i < t$,

$$N(p^{k+i} k_1, p^j) = \varphi(p^s)\varphi(p^j)/k_1.$$

CASE (iv) $f(x) = g(x) = (x - a)^2 \bmod p$

Theorem 6.6. *(One of sixteen cases.) Let $p = 2$ and assume $A = I + E + 2B$, where $E = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B \not\equiv 0$ mod 2. Then $A^2 = I + 2^s C$ for some integer $s \ge 1$ and $C \not\equiv 0$ mod 2 an integral matrix. Finally, suppose that $|A + I| = 0 \ne |A - I|$ with $s = 1$. Then $N(1, 2) = N(2, 2) = 1$, $N(1, 4) = N(4, 4) = 2N(2, 4) = 2$ and if $j \ge 3$, then $N(2, 2^j) = N(2^j, 2^j) = 2N(2^t, 2^j) = 2^{j-1}$, where $1 < t < j$.*

References

[1] Ezra Brown, Directed graphs defined by arithmetic mod n, *Fibonacci Quarterly* **35** (1997), 346–351.

[2] K. Hoffman and R. Kunze, Linear Algebra, Prentice–Hall (1971).

[3] D. Marcus, Number Fields, Springer–Verlag (1987).

[4] Morris Newman, *Integral Matrices*, Academic Press (1972).

Department of Mathematics, Virginia Tech, Blacksburg, Virginia 24061
E-mail address: brown@math.vt.edu

Department of Mathematics, University of North Carolina – Greensboro, Greensboro, North Carolina 27412
E-mail address: tpvaugha@euler.uncg.edu