Investigating Diagonalizable Matrices Modulo m

Dylan Stover

Advisor: Dr. Brian Sittinger

California State University, Channel Islands

1. Introduction

In most introductory courses to Linear Algebra, one works with matrices over a field (usually $\mathbb{R}$ or $\mathbb{C}$), and a major topic from an introductory course concerns diagonalizing a matrix. It is well-known that in this context, this diagonalization, when it exists, is unique up to the order of the diagonal elements. Instead of working over a field, we investigate whether this fact is still true if we work over the ring $\mathbb{Z}_m$, especially in the case where m is not a prime number.

2. Definitions and Notation

- Let $\mathbb{Z}_m = \{0, 1, ..., m-1\}$ denote the ring of integers modulo m.
- Let $M_n(\mathbb{Z}_m)$ denote the set of $n \times n$ matrices whose entries are in $\mathbb{Z}_m$.
- Let $GL_n(\mathbb{Z}_m)$ denote the set of invertible matrices in $M_n(\mathbb{Z}_m)$.
- A is **similar** to B if $A = PBP^{-1}$ where $B \in M_n(\mathbb{Z}_m)$ and $P \in GL_n(\mathbb{Z}_m)$.
- A is **diagonalizable** (over $\mathbb{Z}_m$) if A is similar to a diagonal matrix $D \in M_n(\mathbb{Z}_m)$.
- For notational shorthand to the diagonal matrix $D = \begin{pmatrix} d_1 & 0 & 0 & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 \\ 0 & 0 & d_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & d_n \end{pmatrix}$, we can express this compactly as $D = \text{diag}(d_1, d_2, ..., d_n)$.

3. Unique Diagonalization modulo p^k

We start by examining the case when $m = p^k$ where p is a prime number and $k \in \mathbb{N}$. Since $\mathbb{Z}_p$ is a field, classic results from Linear Algebra readily imply that if $A \in \mathbb{Z}_p$ is diagonalizable over $\mathbb{Z}_p$, then it is unique up to ordering of its diagonal entries. The following theorem extends this result to $\mathbb{Z}_{p^k}$.

Theorem 3.1. *Any diagonalizable matrix over $\mathbb{Z}_{p^k}$ is unique up to ordering of its diagonal entries.*

Proof. Suppose that $D, D' \in M_n(\mathbb{Z}_{p^k})$ are diagonal matrices such that $D' = PDP^{-1}$ for some $P \in GL_n(\mathbb{Z}_{p^k})$. Writing $D = \text{diag}(d_1, \dots, d_n)$, $D' = \text{diag}(d'_1, \dots, d'_n)$, and $P = (p_{ij})$, we see that $D' = PDP^{-1}$ rewritten as $PD = D'P$ yields $p_{ij}d_i = p_{ij}d'_j$ for all i, j.

Since $P \in GL_n(\mathbb{Z}_{p^k})$, we know that $\det P \in \mathbb{Z}^*_{p^k}$, and thus $\det P \not\equiv 0 \bmod p$. However, since $\det P = \sum_{\sigma \in S_n} (-1)^{\text{sgn}(\sigma)} \prod_i p_{i,\sigma(i)}$, and the set of non-units in $\mathbb{Z}_{p^k}$ (which is precisely the subset of elements congruent to 0 mod p) is additively closed, there exists $\sigma \in S_n$ such that $\prod_i p_{i,\sigma(i)} \in \mathbb{Z}^*_{p^k}$ and thus $p_{i,\sigma(i)} \in \mathbb{Z}^*_{p^k}$ for all i.

Then for this choice of σ, it follows that $p_{i,\sigma(i)}d_i = p_{i,\sigma(i)}d'_{\sigma(i)}$ for each i, and since $p_{i,\sigma(i)} \in \mathbb{Z}^*_{p^k}$, we deduce that $d_i = d'_{\sigma(i)}$ for each i. In other words, σ is a permutation of the diagonal entries of D and D', giving us the desired result. □

4. Diagonalization modulo m

The next natural question is whether a diagonalization of a matrix $A \in M_m(\mathbb{Z}_m)$ (if it exists) is unique if m has *more than two* prime divisors. This is not the case.

Example: Consider $\begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} \in M_2(\mathbb{Z}_6)$, which has two distinct diagonalizations

$$\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 5 & 2 \end{pmatrix}^{-1}.$$

An observation that leads to unraveling this surprise is the following. Noting that $6 = 2 \cdot 3$, reducing the two diagonal matrices occurring modulo 6 to the smaller moduli 2 and 3 yields

Diagonal matrix mod 6	Reduction mod 2	Reduction mod 3
$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$
$\begin{pmatrix} 5 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$

By Theorem 3.1, we should expect for the diagonal matrices modulo 2 and 3 to be essentially the same, up to the ordering of the diagonal entries. However, the two diagonalizations have arisen precisely because we used a different diagonal ordering on one of the two reductions.

5. Enumerating Diagonalizable Matrices Modulo m, special case

Noting that we can always consider the reductions of a matrix modulo m to any one of its prime power divisors, one is lead to the following theorem. For technical reasons, we assume that the diagonalization over $\mathbb{Z}_m$ has *distinct* diagonal entries.

Theorem 5.1. *Let $m = \prod_{j=1}^{r} p_j^{k_j}$, where $p_1, \dots, p_r$ are distinct primes. Suppose that $A \in M_n(\mathbb{Z}_m)$ is similar to a diagonal matrix D with distinct diagonal entries. If $D \bmod p^k$ has t_p distinct diagonal entries having respective multiplicities $m_1^{(p)}, \dots, m_{t_p}^{(p)}$ for each $p \mid m$ where $p^k \mid\mid m$, then A has*

$$\frac{1}{n!} \cdot \prod_{p \mid m} \frac{n!}{m_1^{(p)}! \cdot \dots \cdot m_{t_p}^{(p)}!}$$

distinct diagonalizations, up to ordering of diagonal entries, in its similarity class.

Proof. Given a diagonal matrix $D \in M_n(\mathbb{Z}_m)$, we know that for each $p \mid m$ where $p^k \mid\mid m$, $D \bmod p^k$ is unique up to its order of diagonal entries by Theorem 3.1. If we apply the Chinese Remainder Theorem (CRT) to $D \bmod p_1^{k_1}, \dots, D \bmod p_r^{k_r}$ entrywise, we retrieve D. However, if we rearrange the entries in each of matrices, *but not in the same manner*, applying the CRT yields a different diagonal matrix in $M_n(\mathbb{Z}_m)$. Since there are $\prod_{p \mid m} \frac{n!}{m_1^{(p)}! \cdot \dots \cdot m_{t_p}^{(p)}!}$ ways to perform such a rearrangement, and there are $n!$ ways to arrange the entries of the resulting matrix in $M_n(\mathbb{Z}_m)$, the result immediately follows. □

6. Another Example

To illustrate Theorem 5.1, we consider the following matrix $A \in \mathbb{Z}_{360}$:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 \\ 0 & 0 & 313 & 0 \\ 0 & 0 & 0 & 84 \end{pmatrix}.$$

Since 360 has prime factorization $2^3 \cdot 3^2 \cdot 5$, we consider the reductions of A modulo 5, 8, and 9. These are given in the table below.

Reduction mod 5	Reduction mod 8	Reduction mod 9
$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$

Next, we count the number of arrangements of the diagonal entries to A occurring in each of the reductions. For A modulo 5, the diagonal entries can be arranged in $4!$ ways, for A modulo 8, the diagonal entries can be arranged in $\frac{4!}{2!\,2!}$ ways (since it has two diagonal entries both occurring twice), and for A modulo 9, the diagonal entries can be arranged in $\frac{4!}{2!}$ ways. Keeping in mind that A has $4!$ arrangements of its diagonal entries, we conclude that there are

$$\frac{1}{4!} \cdot \left(4! \cdot \frac{4!}{2!\,2!} \cdot \frac{4!}{2!}\right) = 72$$

distinct diagonal matrices belonging in the same similarity class over $\mathbb{Z}_{360}$.

7. Future Directions

- If a square matrix is diagonalizable over $\mathbb{Z}_m$ where m has at least two distinct prime factors and the diagonal matrix has *repeated* diagonal entries, then how many diagonalizations does it have?
- The proof to Theorem 3.1 can readily be adapted to show that any diagonalizable matrix over any commutative *local* ring R (a ring with a unique maximal ideal) is unique up to ordering of its diagonal entries. How much further can we generalize this theorem?
- Working modulo m, assume that a square matrix $A \in M_n(\mathbb{Z}_m)$ admits a "Jordan Canonical Form", that is, A is similar to a block diagonal matrix whose diagonal blocks are either diagonal matrices or have the form of a Jordan matrix

$$\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda \end{pmatrix}.$$

  Under what conditions is this Jordan Canonical Form unique?

References

[1] Brown, *Matrices Over Commutative Rings.* Marcel Dekker, Inc., New York (1993).

[2] Falvey, Hah, Sheppard, Sittinger, Vicente, *Enumerating Diagonalizable Matrices Over $\mathbb{Z}_{p^k}$.* Involve Vol. 13 (2020), No.2, 323-344.