

involve

a journal of mathematics

Enumerating diagonalizable matrices over \mathbb{Z}_{p^k}

Catherine Falvey, Heewon Hah, William Sheppard,
Brian Sittinger and Rico Vicente



Enumerating diagonalizable matrices over \mathbb{Z}_{p^k}

Catherine Falvey, Heewon Hah, William Sheppard,
 Brian Sittinger and Rico Vicente

(Communicated by Stephan Garcia)

Although a good portion of elementary linear algebra concerns itself with matrices over a field such as \mathbb{R} or \mathbb{C} , many combinatorial problems naturally surface when we instead work with matrices over a finite field. As some recent work has been done in these areas, we turn our attention to the problem of enumerating the square matrices with entries in \mathbb{Z}_{p^k} that are diagonalizable over \mathbb{Z}_{p^k} . This turns out to be significantly more nontrivial than its finite-field counterpart due to the presence of zero divisors in \mathbb{Z}_{p^k} .

1. Introduction

A classic problem in linear algebra concerns whether a matrix $A \in M_n(K)$ (where K is a field) is diagonalizable; that is, there exists an invertible matrix $P \in \text{GL}_n(K)$ and a diagonal matrix $D \in M_n(K)$ such that $A = PDP^{-1}$. It is known that if A is diagonalizable, then D is unique up to the order of its diagonal elements. Besides being useful for computing functions of matrices (and therefore often giving a solution to a system of linear differential equations), this problem has applications in the representation of quadratic forms.

If we consider $M_n(K)$ when K is a finite field, one natural problem is to enumerate $\text{Eig}_n(K)$, the set of $n \times n$ matrices over K whose n eigenvalues, counting multiplicity, are in K . Olšavský [2003] initiated this line of inquiry and determined that for any prime p

$$|\text{Eig}_2(\mathbb{F}_p)| = \frac{1}{2}(p^4 + 2p^3 - p^2).$$

More recently, Kaylor and Offner [2014] gave a procedure to enumerate $\text{Eig}_n(\mathbb{F}_q)$, thereby extending Olšavský's work for any n and any finite field \mathbb{F}_q .

Inspired by these works, we turn our attention to $n \times n$ matrices over \mathbb{Z}_{p^k} , where p is a prime and k is a positive integer. More specifically, we investigate the problem of enumerating $\text{Diag}_n(\mathbb{Z}_{p^k})$, the set of $n \times n$ diagonalizable matrices over \mathbb{Z}_{p^k} . This is

MSC2010: 05A05, 05C22, 15A18, 15B33.

Keywords: eigenvalues, matrices, finite commutative rings.

significantly more involved when $k \geq 2$, and many of the difficulties arise from having to carefully consider the zero divisors of \mathbb{Z}_{p^k} , namely any integral multiple of p .

In Section 2, we review the pertinent definitions and notation for working with matrices over commutative rings. Most notably, we give a crucial theorem that essentially states that a diagonalizable matrix over \mathbb{Z}_{p^k} is unique up to the ordering of its diagonal entries. In Section 3, we give the basic procedure for enumerating $\text{Diag}_n(\mathbb{Z}_{p^k})$ and apply it to the case where $n = 2$ in Section 4. In order to deal with the cases where $n \geq 3$ in a systematic manner, we introduce to any diagonal matrix an associated weighted graph in Section 5 that allows us to find $|\text{Diag}_3(\mathbb{Z}_{p^k})|$ and $|\text{Diag}_4(\mathbb{Z}_{p^k})|$ in Sections 6 and 7, respectively. In the final sections, we use our work to find the proportion of matrices that are diagonalizable over \mathbb{Z}_{p^k} and conclude by giving ideas for future research based on the ideas in this article. As far as we understand, all results and definitions from Proposition 3.4 in Section 3 onward are original.

2. Background

We give some definitions from matrix theory over rings that allow us to extend some notions of matrices from elementary linear algebra to those having entries in \mathbb{Z}_{p^k} . For the following definitions, we let R denote a commutative ring with unity. For further details, we refer the interested reader to [Brown 1993].

To fix some notation, let $M_n(R)$ denote the set of $n \times n$ matrices with entries in R . The classic definitions of matrix addition and multiplication as well as determinants generalize in $M_n(R)$ in the expected manner. In general, $M_n(R)$ forms a noncommutative ring with unity I_n , the matrix with 1s on its main diagonal and 0s elsewhere.

Next, we let $\text{GL}_n(R)$ denote the set of invertible matrices in $M_n(R)$; that is,

$$\text{GL}_n(R) = \{A \in M_n(R) : AB = BA = I_n \text{ for some } B \in M_n(R)\}.$$

Note that $\text{GL}_n(R)$ forms a group under matrix multiplication and has the alternative characterization

$$\text{GL}_n(R) = \{A \in M_n(R) : \det A \in R^*\},$$

where R^* denotes the group of units in R . Observe that when R is a field K , we have $K^* = K \setminus \{0\}$; thus we retrieve the classic fact for invertible matrices over K . For this article, we are specifically interested in the case when $R = \mathbb{Z}_{p^k}$, where p is prime and $k \in \mathbb{N}$. Then,

$$\text{GL}_n(\mathbb{Z}_{p^k}) = \{A \in M_n(\mathbb{Z}_{p^k}) : \det A \not\equiv 0 \pmod{p}\};$$

in other words, we can think of an invertible matrix with entries in \mathbb{Z}_{p^k} as having a determinant not divisible by p .

Definition 2.1. We say that $A \in M_n(R)$ is *diagonalizable over R* if A is similar to a diagonal matrix $D \in M_n(R)$; that is, $A = PDP^{-1}$ for some $P \in \text{GL}_n(R)$.

Recall that any diagonalizable matrix over a field is similar to a distinct diagonal matrix that is unique up to ordering of its diagonal entries. Since \mathbb{Z}_{p^k} is *not* a field whenever $k \geq 2$, we now give a generalization of this key result to matrices over \mathbb{Z}_{p^k} . This provides a foundational result that allows us to use the methods from [Kaylor and Offner 2014] to enumerate diagonalizable matrices over \mathbb{Z}_{p^k} . Although we originally came up for a proof for this result, the following elegant proof was suggested to the authors by an anonymous MathOverflow user.¹

Theorem 2.2. Any diagonalizable matrix over \mathbb{Z}_{p^k} is similar to exactly one diagonal matrix that is unique up to the 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 $P \in \text{GL}_n(\mathbb{Z}_{p^k})$. 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 $P \in \text{GL}_n(\mathbb{Z}_{p^k})$, we know that $\det P \in \mathbb{Z}_{p^k}^*$, and thus $\det P \not\equiv 0 \pmod{p}$. However, since

$$\det P = \sum_{\sigma \in S_n} (-1)^{\text{sgn}(\sigma)} \prod_i p_{i, \sigma(i)},$$

and the set of nonunits 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. \square

Remark. Theorem 2.2 does not extend to \mathbb{Z}_m for a modulus m with more than one prime factor. As an example from [Brown 1993], the matrix

$$\begin{pmatrix} 2 & 3 \\ 4 & 3 \end{pmatrix} \in M_2(\mathbb{Z}_6)$$

has two distinct diagonalizations

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

The resulting diagonal matrices are thus similar over \mathbb{Z}_6 although their diagonal entries are not rearrangements of one another.

¹See the response from user 44191 at <https://mathoverflow.net/questions/303634/uniqueness-of-diagonalizing-a-matrix-over-mathbbz-pk>.

3. How to determine $|\text{Diag}_n(\mathbb{Z}_{p^k})|$

We give a procedure that allows us to determine $|\text{Diag}_n(\mathbb{Z}_{p^k})|$, the number of matrices in $M_n(\mathbb{Z}_{p^k})$ that are diagonalizable over \mathbb{Z}_{p^k} . The main idea is to use a generalization of [Kaylor and Offner 2014, Lemma 3.1]. Before stating it, we first fix some notation in the following definition.

Definition 3.1. Let R be a commutative ring with 1, and fix $A \in M_n(R)$.

- The *similarity (conjugacy) class* of A , denoted by $S(A)$, is the set of matrices similar to A :

$$S(A) = \{B \in M_n(R) : B = PAP^{-1} \text{ for some } P \in \text{GL}_n(R)\}.$$

- The *centralizer* of A , denoted by $C(A)$, is the set of invertible matrices that commute with A :

$$C(A) = \{P \in \text{GL}_n(R) : PA = AP\}.$$

Note that $P \in C(A)$ if and only if $A = PAP^{-1}$, and moreover $C(A)$ is a subgroup of $\text{GL}_n(R)$.

Lemma 3.2. Let R be a finite commutative ring. For any $A \in M_n(R)$, we have

$$|S(A)| = \frac{|\text{GL}_n(R)|}{|C(A)|}.$$

Proof. This is proved verbatim as Lemma 3.1 in [Kaylor and Offner 2014] upon replacing a finite field with a finite commutative ring. Alternatively, this is a direct consequence of the orbit-stabilizer theorem where $\text{GL}_n(R)$ is acting on $M_n(R)$ via conjugation. \square

To see how this helps us in $M_n(\mathbb{Z}_{p^k})$, recall by Theorem 2.2 that the similarity class of a given diagonalizable matrix can be represented by a unique diagonal matrix (up to the ordering of diagonal entries). Therefore, we can enumerate $\text{Diag}_n(\mathbb{Z}_{p^k})$ by first enumerating the diagonal matrices in $M_n(\mathbb{Z}_{p^k})$ and then counting how many matrices in $M_n(\mathbb{Z}_{p^k})$ are similar to a given diagonal matrix. Then, Lemma 3.2 yields

$$|\text{Diag}_n(\mathbb{Z}_{p^k})| = \sum_{D \in M_n(\mathbb{Z}_{p^k})} |S(D)| = \sum_{D \in M_n(\mathbb{Z}_{p^k})} \frac{|\text{GL}_n(\mathbb{Z}_{p^k})|}{|C(D)|}, \quad (1)$$

where it is understood that each diagonal matrix D represents a distinct similarity class of diagonal matrices. Observe that diagonal matrices having the same diagonal entries up to order belong to the same similarity class and are counted as different matrices when computing the size of their similarity class.

First, we give a formula for $|\text{GL}_n(\mathbb{Z}_{p^k})|$. As this seems to be surprisingly not well known, we state and give a self-contained proof of this result inspired by [Bollman and Ramírez 1969]; for a generalization, see [Han 2006].

Lemma 3.3. $|\mathrm{GL}_n(\mathbb{Z}_{p^k})| = p^{n^2(k-1)} \prod_{l=1}^n (p^n - p^{l-1}).$

Proof. First, we compute $|\mathrm{GL}_n(\mathbb{Z}_p)|$ by enumerating the possible columns of its matrices. For $A \in \mathrm{GL}_n(\mathbb{Z}_p)$, there are $p^n - 1$ choices for the first column of A , as the zero column vector is never linearly independent. Next, we fix $l \in \{2, 3, \dots, n\}$. After having chosen the first $l - 1$ columns, there are $(p^n - 1) - (p^{l-1} - 1) = p^n - p^{l-1}$ choices for the l -th column, because we want these l columns to be linearly independent over \mathbb{Z}_p (and there are p multiples for each of the first $l - 1$ columns). Therefore, we conclude that

$$|\mathrm{GL}_n(\mathbb{Z}_p)| = \prod_{l=1}^n (p^n - p^{l-1}).$$

Hereafter, we assume that $k \geq 2$. Consider the mapping $\psi : M_n(\mathbb{Z}_{p^k}) \rightarrow M_n(\mathbb{Z}_p)$ defined by $\psi(A) = A \bmod p$; note that ψ is a well-defined (due to $p \mid p^k$) surjective ring homomorphism. Moreover, since

$$\ker \psi = \{A \in M_n(\mathbb{Z}_{p^k}) : \psi(A) = 0 \bmod p\}$$

(so that every entry in such a matrix is divisible by p), we deduce that

$$|\ker \psi| = \left(\frac{p^k}{p}\right)^{n^2} = p^{(k-1)n^2}.$$

Then, restricting ψ to the respective groups of invertible matrices, the first isomorphism theorem yields

$$\frac{|\mathrm{GL}_n(\mathbb{Z}_{p^k})|}{|\ker \psi|} \cong |\mathrm{GL}_n(\mathbb{Z}_p)|.$$

Therefore, we conclude that

$$|\mathrm{GL}_n(\mathbb{Z}_{p^k})| = |\ker \psi| |\mathrm{GL}_n(\mathbb{Z}_p)| = p^{n^2(k-1)} \prod_{l=1}^n (p^n - p^{l-1}). \quad \square$$

We next turn our attention to the problem of enumerating the centralizer of a diagonal matrix in \mathbb{Z}_{p^k} .

Proposition 3.4. *Let $D \in M_n(\mathbb{Z}_{p^k})$ be a diagonal matrix whose distinct diagonal entries $\lambda_1, \dots, \lambda_g$ have multiplicities m_1, \dots, m_g , respectively. Then,*

$$|C(D)| = \left(\prod_{i=1}^g |\mathrm{GL}_{m_i}(\mathbb{Z}_{p^k})| \right) \left(\prod_{j=2}^g \prod_{i=1}^{j-1} p^{2m_i m_j l_{ij}} \right),$$

where l_{ij} is the nonnegative integer satisfying $p^{l_{ij}} \parallel (\lambda_i - \lambda_j)$ for each i and j ; that is,

$$\lambda_i - \lambda_j = r p^{l_{ij}} \quad \text{for some } r \in \mathbb{Z}_{p^{k-l_{ij}}}^*.$$

Proof. Assume without loss of generality that all matching diagonal entries of D are grouped together; that is, we can think of each λ_i with multiplicity m_i as having its own $m_i \times m_i$ diagonal block of the form $\lambda_i I_{m_i}$ within D .

To find the centralizer of D , we need to account for all $A \in \text{GL}_n(\mathbb{Z}_{p^k})$ such that $AD = DA$. Writing $A = (A_{ij})$, where A_{ij} is an $m_i \times m_j$ block, computing the necessary products and equating like entries yields

$$\lambda_i A_{ij} = \lambda_j A_{ij}.$$

If $i \neq j$, then $(\lambda_i - \lambda_j)A_{ij} \equiv 0 \pmod{p^k}$. Therefore, $A_{ij} \equiv 0 \pmod{p^{k-l_{ij}}}$, and thus $A_{ij} \equiv 0 \pmod{p}$. Observe that this gives $p^{l_{ij}}$ possible values for each entry in A_{ij} (and similarly for those in A_{ji}).

Therefore, A is congruent to a block diagonal matrix modulo p with blocks A_{ii} having dimensions $m_i \times m_i$ for each $i \in \{1, \dots, g\}$. Finally since $A \in \text{GL}_n(\mathbb{Z}_{p^k})$, this means that $A_{ii} \in \text{GL}_{m_i}(\mathbb{Z}_{p^k})$ for all i . With this last observation, the formula for $|C(D)|$ now follows immediately. \square

Proposition 3.4 motivates the following classification of diagonal matrices in \mathbb{Z}_{p^k} .

Definition 3.5. Let $D \in M_n(\mathbb{Z}_{p^k})$ be a diagonal matrix whose distinct diagonal entries $\lambda_1, \dots, \lambda_g$ have multiplicities m_1, \dots, m_g , respectively. The *type* of D is given by the following two quantities:

- the partition $n = m_1 + \dots + m_g$,
- the set $\{l_{ij}\}$ indexed over all $1 \leq i < j \leq g$, where $p^{l_{ij}} \parallel (\lambda_j - \lambda_i)$.

Then we say that two diagonal matrices $D, D' \in M_n(\mathbb{Z}_{p^k})$ have the *same type* if and only if D and D' share the same partition of n , and there exists a permutation $\sigma \in S_n$ such that $l_{ij} = l'_{\sigma(i)\sigma(j)}$ for all $1 \leq i < j \leq g$. We denote the set of all distinct types of diagonal $n \times n$ matrices by $\mathcal{T}(n)$.

Example. Consider the following three diagonal matrices from $M_3(\mathbb{Z}_8)$:

$$D_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix}, \quad D_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad D_4 = \begin{pmatrix} 7 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 7 \end{pmatrix}.$$

Since D_1 has partition $1 + 1 + 1$, while D_2, D_3 , and D_4 have the partition $2 + 1$, D_1 does not have the same type as any of D_2, D_3 , and D_4 . Moreover, D_2 and D_3 do not have the same type, because $2^2 \parallel (5 - 1)$, while $2^1 \parallel (3 - 1)$. However, D_3 and D_4 have the same type, because they share the same partition $2 + 1$ and 2^1 exactly divides both $3 - 1$ and $7 - 5$.

It is easy to verify that if D and D' are two $n \times n$ diagonal matrices of the same type, then $|C(D)| = |C(D')|$ and thus $|S(D)| = |S(D')|$. Consequently for any type T , define $c(T)$ and $s(T)$ by $c(T) = |C(D)|$ and $s(T) = |S(D)|$, where D is

any matrix of type T . Then, letting $t(T)$ denote the number of diagonal matrices (up to permutations of the diagonal entries) having type T , we can rewrite (1) as

$$|\text{Diag}_n(\mathbb{Z}_{p^k})| = \sum_{T \in \mathcal{T}(n)} t(T) \frac{|\text{GL}_n(\mathbb{Z}_{p^k})|}{c(T)}. \quad (2)$$

4. Enumerating the 2×2 diagonalizable matrices

We now illustrate our procedure for determining the value of $|\text{Diag}_2(\mathbb{Z}_{p^k})|$.

Theorem 4.1. *The number of 2×2 matrices with entries in \mathbb{Z}_{p^k} that are diagonalizable over \mathbb{Z}_{p^k} is*

$$|\text{Diag}_2(\mathbb{Z}_{p^k})| = p^k + \frac{p^{k+1}(p^2 - 1)(p^{3k} - 1)}{2(p^3 - 1)}.$$

Proof. In order to find $|\text{Diag}_2(\mathbb{Z}_{p^k})|$, we need to enumerate all of the 2×2 diagonal matrix types. First of all, there are two possible partitions of 2, namely 2 and $1 + 1$. The trivial partition yields one distinct type of diagonal matrix

$$T_1 = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in \mathbb{Z}_{p^k} \right\},$$

which consists of the 2×2 scalar matrices. Since there are p^k choices for λ , we have $t(T_1) = p^k$. Moreover $c(T_1) = |\text{GL}_2(\mathbb{Z}_{p^k})|$, because any invertible matrix commutes with a scalar matrix.

The nontrivial partition $2 = 1 + 1$ yields the remaining k distinct types of matrices that we index by $i \in \{0, 1, \dots, k - 1\}$:

$$T_2^{(i)} = \left\{ \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} : p^i \parallel (\lambda_1 - \lambda_2) \right\}.$$

Fix $i \in \{0, 1, \dots, k - 1\}$; we now enumerate $t(T_2^{(i)})$ and $c(T_2^{(i)})$. For $t(T_2^{(i)})$, we first observe that there are p^k choices for λ_1 . To find the number of choices for λ_2 , observe that $\lambda_1 - \lambda_2 \equiv r p^i \pmod{p^k}$ for some unique $r \in (\mathbb{Z}_{p^{k-i}})^*$. Hence, there are $\phi(p^{k-i})$ choices for r and thus for λ_2 . (As a reminder, ϕ denotes the Euler phi function, and $\phi(p^l) = p^{l-1}(p - 1)$.) Since swapping λ_1 and λ_2 does not change the similarity class of the diagonal matrix, we conclude that

$$t(T_2^{(i)}) = \frac{p^k \phi(p^{k-i})}{2!}.$$

Next, applying Proposition 3.4 yields

$$c(T_2^{(i)}) = p^{2i} \phi(p^k)^2.$$

Finally, we use (2) to enumerate the 2×2 diagonal matrices and conclude that

$$\begin{aligned}
 |\text{Diag}_2(\mathbb{Z}_{p^k})| &= t(T_1) \frac{|\text{GL}_n(\mathbb{Z}_{p^k})|}{c(T_1)} + \sum_{i=0}^{k-1} t(T_2^{(i)}) \frac{|\text{GL}_n(\mathbb{Z}_{p^k})|}{c(T_2^{(i)})} \\
 &= p^k + \frac{p^k}{2} \frac{p^{4(k-1)}(p^2-1)(p^2-p)}{\phi(p^k)^2} \sum_{i=0}^{k-1} \frac{\phi(p^{k-i})}{p^{2i}} \\
 &= p^k + \frac{p^k}{2} \frac{p^{4(k-1)}(p^2-1)(p^2-p)}{(p^{k-1}(p-1))^2} \sum_{i=0}^{k-1} \frac{p^{k-i-1}(p-1)}{p^{2i}} \\
 &= p^k + \frac{p^{4k-2}(p^2-1)}{2} \sum_{i=0}^{k-1} \frac{1}{p^{3i}} \\
 &= p^k + \frac{p^{4k-2}(p^2-1)}{2} \frac{1-p^{-3k}}{1-p^{-3}} \quad (\text{using the geometric series}) \\
 &= p^k + \frac{p^{k+1}(p^2-1)(p^{3k}-1)}{2(p^3-1)}. \quad \square
 \end{aligned}$$

Remarks. In the case where $k = 1$, the formula reduces to $\frac{1}{2}(p^4 - p^2 + p)$, which can be found at the end of Section 3 in [Kaylor and Offner 2014] after you remove the contributions from the 2×2 Jordan block case. Moreover, for the diagonal matrix types corresponding to the nontrivial partition and $i \geq 1$, we are dealing with differences of diagonal entries yielding zero divisors in \mathbb{Z}_{p^k} ; these scenarios never occur when $k = 1$ because \mathbb{Z}_p is a field.

5. Enumerating $n \times n$ diagonal matrices of a given type

Representing a diagonal matrix with a valuation graph. As we increase the value of n , the enumeration of $n \times n$ diagonalizable matrices over \mathbb{Z}_{p^k} becomes more involved, because the number of distinct types becomes increasingly difficult to catalog. The difficulties come both from the powers of p dividing the differences of the diagonal entries of the matrix as well as the increasing number of partitions of n . In order to aid us in classifying diagonal matrices into distinct types, we introduce an associated graph to help visualize these scenarios.

Let $D \in M_n(\mathbb{Z}_{p^k})$ be diagonal with distinct diagonal entries $\lambda_1, \dots, \lambda_g \in \mathbb{Z}_{p^k}$. Ordering the elements in \mathbb{Z}_{p^k} by $0 < 1 < 2 < \dots < p^k - 1$, we can assume without loss of generality that $\lambda_1 < \lambda_2 < \dots < \lambda_g$ (since D is similar to such a matrix by using a suitable permutation matrix as the change of basis matrix). Associated to D , we define its associated weighted complete graph G_D (abbreviated as G when no ambiguity can arise) as follows: we label its g vertices with the diagonal entries $\lambda_1, \lambda_2, \dots, \lambda_g$, and given the edge between the vertices λ_i and λ_j , we define its weight l_{ij} as the unique nonnegative integer satisfying $p^{l_{ij}} \parallel (\lambda_i - \lambda_j)$.

Definition 5.1. Let $D \in M_n(\mathbb{Z}_{p^k})$ be diagonal. We call the weighted complete graph G associated to D as constructed above the *valuation graph* of D .

The following fundamental property of such graphs justifies why we call these valuation graphs.

Proposition 5.2 (triangle inequality). *Let G be a valuation graph. Given vertices λ_a, λ_b , and λ_c in G and edges E_{ab}, E_{ac} , and E_{bc} , the weights satisfy $l_{bc} \geq \min\{l_{ab}, l_{ac}\}$. In particular, $l_{bc} = \min\{l_{ab}, l_{ac}\}$ if $l_{ab} \neq l_{ac}$.*

Proof. By hypothesis, we know that l_{ab} and l_{ac} are the biggest nonnegative integers satisfying

$$\lambda_a - \lambda_b = rp^{l_{ab}} \quad \text{and} \quad \lambda_a - \lambda_c = sp^{l_{ac}} \quad \text{for some } r, s \in \mathbb{Z}_{p^k}^*.$$

Without loss of generality, assume that $l_{ab} \geq l_{ac}$. Then, we obtain

$$\lambda_b - \lambda_c = (\lambda_a - \lambda_c) - (\lambda_a - \lambda_b) = p^{l_{ac}}(s - rp^{l_{ab}-l_{ac}}).$$

If $l_{ab} > l_{ac}$, then $(s - rp^{l_{ab}-l_{ac}}) \in \mathbb{Z}_{p^k}^*$, and if $l_{ab} = l_{ac}$ then $s - r$ may or may not be a zero divisor in \mathbb{Z}_{p^k} . The claim now immediately follows. \square

Observe that since the valuation graph arises from a diagonal matrix in $M_n(\mathbb{Z}_{p^k})$, it is clear that its weights can only attain integral values between 0 and $k - 1$ inclusive. In fact, we can give another restriction on the possible values of its weights.

Lemma 5.3. *A valuation graph G on g vertices has no more than $g - 1$ weights.*

Proof. We prove this by induction on the number of vertices g . This claim is true for $g = 2$, because such a graph has exactly one weight. Next, we assume that the claim is true for any valuation graph on g vertices, and consider a valuation graph G with vertices $\lambda_1, \dots, \lambda_{g+1}$. By the inductive hypothesis, the valuation subgraph H of G with vertices $\lambda_1, \dots, \lambda_g$ has no more than $g - 1$ weights. It remains to consider the weights of the edges from these vertices to the remaining vertex λ_{g+1} . If none of these edges have any of the $g - 1$ weights of H , then we are done. Otherwise, suppose that one of these edges (call it E) has an additional weight. Then for any edge E' other than E that has λ_{g+1} as a vertex, the triangle inequality (Proposition 5.2) implies that E' has no new weight. Hence, G has no more than $(g - 1) + 1 = g$ weights as required, and this completes the inductive step. \square

We know that for any diagonal matrix $D \in M_n(\mathbb{Z}_{p^k})$, its valuation graph G satisfies the triangle inequality. Moreover, any complete graph on n vertices satisfying the triangle inequality necessarily corresponds to a collection of diagonal matrices with distinct diagonal entries in $M_n(\mathbb{Z}_{p^k})$ as long as there are at most $n - 1$ weights and the maximal weight is at most $k - 1$. Moreover, such a graph also corresponds to a collection of diagonal matrices with nondistinct diagonal entries in $M_N(\mathbb{Z}_{p^k})$, where N is the sum of these multiplicities.

Enumerating diagonalizable matrices with a given valuation graph. Throughout this section, we assume that the diagonal matrix in $M_n(\mathbb{Z}_{p^k})$ has distinct diagonal entries. Given its valuation graph G , we construct a specific kind of spanning tree that will aid us in enumerating the diagonal matrices in $M_n(\mathbb{Z}_{p^k})$ having valuation graph G . In a sense, such a spanning tree concisely shows the dependencies among the diagonal entries of a given diagonal matrix.

Proposition 5.4. *Given a diagonal matrix $D \in M_n(\mathbb{Z}_{p^k})$ with distinct diagonal entries having valuation graph G , there exists a spanning tree $T \subset G$ from which we can uniquely reconstruct G . We call T a permissible spanning tree of G .*

Proof. Suppose that G is a valuation graph on n vertices with r distinct weights a_1, a_2, \dots, a_r listed in increasing order. In order to construct a permissible spanning tree for G , we consider the following construction.

For each weight a_i with $1 \leq i \leq r$, define G_{a_i} to be the subgraph of G consisting of the edges with weight at most a_i along with their respective vertices. From the definition of a weight, we immediately see that $G_{a_1} \supseteq G_{a_2} \supseteq \dots \supseteq G_{a_r}$. Moreover, Proposition 5.2 implies that each connected component of G_{a_i} is a complete subgraph of G .

To use these subgraphs to construct a permissible spanning tree for G , we start with the edges in G_{a_r} . For each connected component of G_{a_r} , we select a spanning tree and include all of their edges into the edge set E . Next, we consider the edges in $G_{a_{r-1}}$. For each connected component of $G_{a_{r-1}}$, we select a spanning tree that includes the spanning tree from the previous step. We inductively repeat this process until we have added any pertinent edges from G_{a_1} . (Note that since G_{a_1} contains only one connected component, T must also be connected.) The result is a desired permissible spanning tree T for our valuation graph G .

Next, we show how to uniquely reconstruct the valuation graph G from T . To aid in this procedure, we say that the *completing edge* of two edges e_1, e_2 in G that share a vertex is the edge e_3 which forms a complete graph K_3 with e_1 and e_2 .

Start by looking at the edges having the largest weight a_r in T . If two edges with weight a_r share a vertex, then their completing edge in G must also have weight a_r by the maximality of a_r . Upon completing this procedure, there can be no other edges in G of weight a_r , as this would violate the construction of T .

Next consider the edges having weight a_{r-1} (if they exist). For any two edges of weight a_{r-1} that share a vertex, their completing edge must have weight a_{r-1} or a_r by the triangle inequality. If the completing edge has weight a_r , then we have already included this edge in the previous step. Otherwise, we conclude that the completing edge must have weight a_{r-1} .

Continuing this process to the lowest edge coloring a_1 , we reconstruct G as desired. \square

We now return to the problem of enumerating diagonal $n \times n$ matrices over \mathbb{Z}_{p^k} of a given type. We begin with the case that $A \in M_n(\mathbb{Z}_{p^k})$ is a diagonal matrix over \mathbb{Z}_{p^k} with distinct diagonal entries. Let G be its associated valuation graph with r distinct weights a_1, a_2, \dots, a_r .

Definition 5.5. Let T be a permissible spanning tree of a valuation graph G . We say that a subset of edges in T all with weight a_t are *linked* if there exists a subtree S of T containing these edges such that each edge in S has weight at least a_t .

We use the notion of linked edges to partition the set of edges from our permissible tree T beyond their weights as follows. Let L^t denote the set of edges in T with weight a_t . Then, L^t decomposes into pairwise disjoint sets $L_1^t, \dots, L_{\ell(t)}^t$ for some positive integer $\ell(t)$, where each L_j^t is a maximal subset of linked edges from L^t .

Definition 5.6. Let T be a permissible spanning tree for a given valuation graph G . For a given weight a_t , we say that $L_1^t, \dots, L_{\ell(t)}^t$ are the *linked cells* of the weight a_t .

Theorem 5.7. Let G be a valuation graph having r distinct weights a_1, a_2, \dots, a_r listed in increasing order, and let T be a permissible spanning tree of G with linked cells L_j^t . Then, the total number of diagonal matrix classes having distinct diagonal entries in $M_n(\mathbb{Z}_{p^k})$ with an associated valuation graph isomorphic to G equals

$$\frac{p^k}{|\text{Aut}(G)|} \prod_{t=1}^r \prod_{j=1}^{\ell(t)} \prod_{i=1}^{|L_j^t|} \phi_i(p^{k-a_t}),$$

where $\phi_i(p^j) = p^j - ip^{j-1}$, and $\text{Aut}(G)$ denotes the set of weighted graph automorphisms of G .

Proof. Fix a valuation graph G . The key idea is to consider the edges of its permissible spanning tree via linked cells, one weight at a time in descending order. Throughout the proof, we use the following convention: if an edge E has vertices λ_1, λ_2 with $\lambda_2 > \lambda_1$, we refer to the value $\lambda_2 - \lambda_1$ as the *edge difference* associated with E .

First consider the edges in the linked cell of the maximal weight a_r . Without loss of generality, we start with the edges in L_1^r . Since a_r is maximal, we know that L_1^r is itself a tree. For brevity, we let $m = |L_1^r|$. Then, L_1^r has m edges connecting its $m+1$ vertices. We claim that there are $\prod_{i=1}^m \phi_i(p^{k-a_r})$ ways to label the values of the edge differences.

To show this, we start by picking an edge in L_1^r , and let λ_1 and λ_2 denote its vertices. Since $\lambda_2 - \lambda_1 = s_1 p^{a_r}$ for some $s_1 \in \mathbb{Z}_{p^{k-a_r}}^*$, we see that $\lambda_2 - \lambda_1$ can attain $\phi(p^{k-a_r}) = \phi_1(p^{k-a_r})$ distinct values. Next, we pick a second edge in L_1^r that connects to either λ_1 or λ_2 ; without loss of generality (relabeling vertices as needed), suppose it is λ_2 . Letting λ_3 denote the other vertex of this edge, $\lambda_3 - \lambda_2 = s_2 p^{a_r}$

for some $s_2 \in \mathbb{Z}_{p^{k-a_r}}^*$. However because a_r is the maximal weight in G , the edge connecting λ_1 and λ_3 also has weight a_r . On the other hand, we have

$$\lambda_3 - \lambda_1 = (\lambda_3 - \lambda_2) + (\lambda_2 - \lambda_1) = (s_2 + s_1)p^{a_r}, \quad \text{where } s_2 + s_1 \in \mathbb{Z}_{p^{k-a_r}}^*.$$

Hence, $s_2 \not\equiv -s_1 \pmod{p^{k-a_r}}$, and therefore there are $\phi_1(p^{k-a_r}) - p^{k-a_r-1} = \phi_2(p^{k-a_r})$ possible values for s_2 . Repeating this procedure, we can assign $\phi_i(p^{k-a_r})$ values to the difference of the vertices from the i -th edge in L_1^r . Now the claim immediately follows.

The preceding discussion applies to any of the linked cells of weight a_r , because edges in distinct linked cells never share a common vertex. Hence, we conclude that the number of possible values of edge differences in L^r equals

$$\prod_{j=1}^{\ell(r)} \prod_{i=1}^{|L_j^r|} \phi_i(p^{k-a_r}).$$

Next, suppose that we have enumerated all edge differences from all linked cells having weights a_{t+1}, \dots, a_r for some fixed t . We now consider linked cells for the weight a_t . The procedure proceeds just as before, with the only difference being that two edges of any weight lower than a_r may be linked via some subtree of T containing other higher weights. However this presents no new difficulties.

Fix a linked cell with weight a_t and choose a first edge with vertices λ_{c_1} and λ_{c_2} . As above, this edge corresponds to one of $\phi_1(p^{k-a_t})$ possible differences between values λ_{c_1} and λ_{c_2} . Given another edge linked to the aforementioned edge in this linked cell, it either shares or does not share a vertex with the first edge. We consider these cases separately.

First, suppose the two edges share a common vertex λ_{c_2} . Then as in the previous case, the connecting edge between λ_{c_1} and λ_{c_3} must have weight at least a_t (as this edge otherwise has weight greater than a_t and such vertices have been previously considered), and thus we can choose the value for $\lambda_{c_3} - \lambda_{c_2}$ in $\phi_2(p^{k-a_t})$ ways.

Alternatively, suppose that the two edges are connected through already established edges of higher weights on the vertices $\lambda_{d_1}, \lambda_{d_2}, \dots, \lambda_{d_s}$. Without loss of generality, assume that the vertices λ_{c_1} and λ_{c_4} are the initial and terminal vertices, respectively, in this second edge. We know that $\lambda_{c_2} - \lambda_{c_1} = rp^{k-a_t}$ and $\lambda_{c_4} - \lambda_{c_3} = r'p^{a_t}$ for some $r, r' \in \mathbb{Z}_{p^{k-a_t}}^*$. Also since the edges connecting λ_{c_2} to λ_{d_1} , λ_{d_s} to λ_{c_3} , and λ_{d_i} to λ_{d_j} for all $1 \leq i < j \leq s$ have weights higher than a_t , it follows that

$$0 \equiv \lambda_{d_1} - \lambda_{c_2} \equiv \lambda_{c_3} - \lambda_{d_s} \equiv \lambda_{d_j} - \lambda_{d_i} \pmod{p^{a_t+1}}$$

and these observations give us

$$\begin{aligned} \lambda_{c_4} - \lambda_{c_1} &\equiv (\lambda_{c_2} - \lambda_{c_1}) + (\lambda_{d_1} - \lambda_{c_2}) + (\lambda_{d_2} - \lambda_{d_1}) + \dots + (\lambda_{c_3} - \lambda_{d_s}) + (\lambda_{c_4} - \lambda_{c_3}) \\ &\equiv (r + r')p^{a_t} \pmod{p^{a_t+1}}. \end{aligned}$$

However, by an inductive use of the triangle inequality, we see that the edge directly connecting c_1 and c_4 must have weight a_t . Thus, $r + r' \not\equiv 0 \pmod{p}$, and the number of permissible choices for r' is therefore

$$p^{k-a_t} - 2p^{k-a_t-1} = \phi_2(p^{k-a_t}).$$

Continuing this process, we can see that when we add the i -th edge in this linked cell (if it exists), we can find a path between it and the previous $i - 1$ edges in T sharing the same linked cell, giving $\phi_i(p^{k-a_t})$ choices for the corresponding edge differences.

At this point we have considered every edge in T . The number of possible edge differences among all of the edges in T equals

$$\prod_{t=1}^r \prod_{j=1}^{\ell(t)} \prod_{i=1}^{|L_j^t|} \phi_i(p^{k-a_t}).$$

In summary, we have specified the number of values that the differences of the vertices to each of the edges in our permissible tree can attain. Consequently, as soon as we specify the value of one vertex, in which there are p^k possible choices, we have uniquely determined (by our work above) the values of the remaining vertices through their differences. Therefore, the number of possible diagonal matrices with the given valuation graph equals

$$p^k \prod_{t=1}^r \prod_{j=1}^{\ell(t)} \prod_{i=1}^{|L_j^t|} \phi_i(p^{k-a_t}).$$

Finally, we note that permuting the order of the diagonal entries of any diagonal matrix associated with G yields a valuation graph isomorphic to G . Since these correspond to the weighted graph automorphisms of G , dividing our last formula by $|\text{Aut}(G)|$ yields the desired enumeration formula. \square

Remark. Note that the group of weighted automorphisms of G is a subgroup of all automorphisms (under composition of isomorphisms) of the corresponding unweighted graph version of G . Since G is a complete graph with n vertices, we know that there are $|S_n| = n!$ unweighted graph automorphisms of G (which can be represented by $n \times n$ permutation matrices). Then, Lagrange's theorem for groups implies that $|\text{Aut}(G)| = n!/\sigma(G)$, where $\sigma(G) = [S_n : \text{Aut}(G)]$ denotes the number of vertex permutations yielding nonisomorphic valuation graphs from G . In this manner, one can determine the value of $|\text{Aut}(G)|$ by directly computing $\sigma(G)$.

So far, Theorem 5.7 allows us to enumerate diagonal matrices with distinct diagonal entries with an associated valuation graph. The following proposition addresses how to extend this theorem to also enumerate diagonal matrices whose diagonal entries are not distinct.

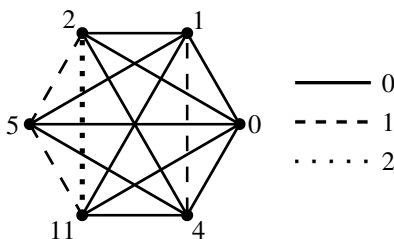


Figure 1. The valuation graph G corresponding to D .

Proposition 5.8. Let $D \in M_n(\mathbb{Z}_{p^k})$ be a diagonal matrix with distinct diagonal entries $\lambda_1, \dots, \lambda_g$, and let $D' \in M_g(\mathbb{Z}_{p^k})$ be the corresponding diagonal matrix with (distinct) diagonal entries $\lambda_1, \dots, \lambda_g$. If D has exactly n_m distinct $m \times m$ diagonal blocks for each $m \in \{1, 2, \dots, g\}$, then

$$t(T) = \frac{g!}{n_1! \cdots n_g!} t(T'),$$

where T and T' are the types of D and D' , respectively.

Proof. Since we know by hypothesis that D and D' share the same number of distinct diagonal entries, it suffices to count the number of ways to arrange the diagonal blocks (each of which is distinguished by a different scalar on their respective diagonals) in D . Since the number of ways of arranging these diagonal blocks in D equals $g!/(n_1! \cdots n_g!)$, the conclusion of this theorem is now an immediate consequence. \square

Now that we have Theorem 5.7 and Proposition 5.8 at our disposal, we are more than ready to enumerate the diagonalizable $n \times n$ matrices in the cases where $n = 3$ and 4; this we address in the next two sections. Before doing this, we would like to put our theory of valuation graphs into perspective by giving an example that illustrates the theory we have developed for the valuation graph.

Example. Consider the diagonal matrix $D \in M_6(\mathbb{Z}_{3^3})$ whose diagonal entries are 0, 1, 2, 4, 5, and 11. Then, its corresponding valuation graph G is depicted in Figure 1. Observe the number of distinct weights in G is 3, consistent with Lemma 5.3, and that the highest edge weight is 2.

Next, we give examples of permissible spanning trees for G and partition their edges into linked cells. Figure 2 shows three permissible spanning trees T_1 , T_2 , T_3 for G and their linked cells L_1^1 , L_1^2 , L_2^2 , and L_1^3 .

Although each of these spanning trees have different degrees, they all have the same edge decomposition into linked cells. Thus, we can use any of these permissible spanning trees to enumerate the number of similarity classes of diagonal matrices sharing G as their valuation graph. To this end, it remains to compute

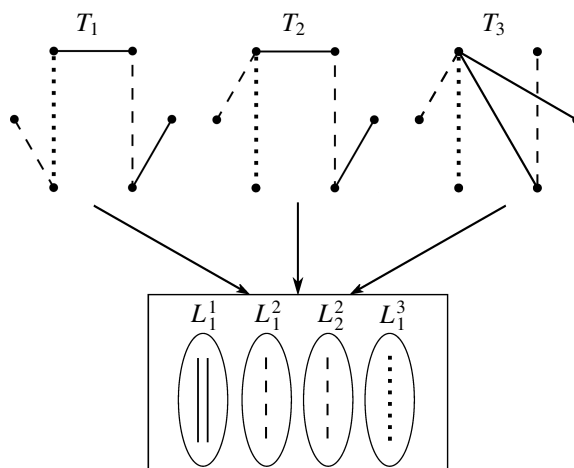


Figure 2. Three permissible spanning trees for G and their linked cells.

$|\text{Aut}(G)|$. Since we can permute the vertices 2 and 11, as well as the vertices 1 and 4 without altering G , this implies $|\text{Aut}(G)| = 2! 2!$. Therefore by Theorem 5.7, the number of similarity classes of diagonal matrices with valuation graph G equals

$$\frac{3^3}{2! 2!} \prod_{t=0}^2 \prod_{j=1}^{\ell(t)} \prod_{i=1}^{|L_j^t|} \phi_i(3^{3-t}) = \frac{27}{4} \phi_1(3^3) \phi_2(3^3) \phi_1(3^2) \phi_1(3^2) \phi_1(3^1) = 78732.$$

6. Enumerating the 3×3 diagonalizable matrices

Theorem 6.1. *The number of 3×3 matrices with entries in \mathbb{Z}_{p^k} that are diagonalizable over \mathbb{Z}_{p^k} is*

$$|\text{Diag}_3(\mathbb{Z}_{p^k})| = p^k + \frac{p^{k+2}(p^3-1)(p^{5k}-1)}{p^5-1} + \frac{p^{k+3}(p^3-1)(p-2)(p+1)(p^{8k}-1)}{6(p^8-1)} + \frac{p^{k+3}(p^2-1)}{2} \left(\frac{p^{8k}-p^8}{p^8-1} - \frac{p^{5k}-p^5}{p^5-1} \right).$$

Proof. We first enumerate all of the 3×3 diagonal matrix types. There are three partitions of 3, namely 3, $2 + 1$, and $1 + 1 + 1$. The trivial partition yields the type of scalar matrices

$$T_1 = \left\{ \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix} : \lambda \in \mathbb{Z}_{p^k} \right\}.$$

As with this type of 2×2 scalar diagonal matrices, we have $t(T_1) = p^k$ and $c(T_1) = |\text{GL}_3(\mathbb{Z}_{p^k})|$.

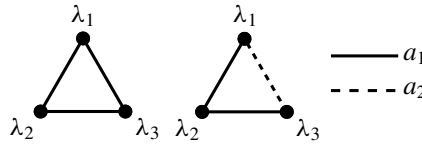


Figure 3. Two valuation graph classes in the 3×3 case.

The partition $3 = 2 + 1$ comprises k distinct types as $i \in \{0, 1, \dots, k-1\}$:

$$T_2^{(i)} = \left\{ \begin{pmatrix} \lambda_1 & & \\ & \lambda_1 & \\ & & \lambda_2 \end{pmatrix} : p^i \parallel (\lambda_1 - \lambda_2) \right\}.$$

Proposition 5.8 relates these types to the nonscalar types of 2×2 diagonal matrices, and thus

$$t(T_2^{(i)}) = \frac{2!}{1!1!} \frac{p^k \phi(p^{k-i})}{2!} = p^k \phi(p^{k-i}).$$

Next, Proposition 3.4 gives us $c(T_2^{(i)}) = \phi(p^k) \cdot |\mathrm{GL}_2(\mathbb{Z}_{p^k})| \cdot p^{4i}$.

Finally, the partition $3 = 1 + 1 + 1$ comprises two distinct classes of diagonal matrix types that we concisely give by their respective valuation graphs in Figure 3.

For the first valuation graph, let $i \in \{0, 1, \dots, k-1\}$ denote the common weight of the three edges on the first valuation graph given above. Letting $T_{3a}^{(i)}$ denote this type, Theorem 5.7 yields

$$t(T_{3a}^{(i)}) = \frac{p^k \phi(p^{k-i}) \phi_2(p^{k-i})}{3!},$$

and Proposition 3.4 gives us $c(T_{3a}^{(i)}) = \phi(p^k)^3 p^{6i}$.

For the second valuation graph, let i and j denote the weights in the second valuation graph given above; note that $i \in \{0, \dots, k-2\}$ and $j \in \{i+1, \dots, k-1\}$. Letting $T_{3b}^{(i,j)}$ denote this type, Theorem 5.7, gives us

$$t(T_{3b}^{(i,j)}) = \frac{p^k \phi(p^{k-i}) \phi(p^{k-j})}{2!},$$

and Proposition 3.4 yields $c(T_{3b}^{(i,j)}) = \phi(p^k)^3 p^{4i+2j}$.

Finally, we use (2) to enumerate the 3×3 diagonal matrices and conclude that

$$\begin{aligned} |\mathrm{Diag}_3(\mathbb{Z}_{p^k})| &= p^k + \frac{p^{k+2}(p^3-1)(p^{5k}-1)}{p^5-1} + \frac{p^{k+3}(p^3-1)(p-2)(p+1)(p^{8k}-1)}{6(p^8-1)} \\ &\quad + \frac{p^{k+3}(p^2-1)}{2} \left(\frac{p^{8k}-p^8}{p^8-1} - \frac{p^{5k}-p^5}{p^5-1} \right). \quad \square \end{aligned}$$

7. Enumerating the 4×4 diagonalizable matrices

We first address the 4×4 diagonal matrices with repeated diagonal entries. By using Propositions 3.4 and 5.8, we obtain the results in the following tables. Table 1 deals with the cases where there are at most two distinct diagonal entries.

In Table 2, we consider the more involved case where a given diagonal matrix has three distinct diagonal entries.

type T	valuation graph	$t(T)$	$c(T)$
$\begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & \lambda & \\ & & & \lambda \end{pmatrix}$	$\bullet \lambda$	p^k	$ \mathrm{GL}_4(\mathbb{Z}_{p^k}) $
$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_1 & & \\ & & \lambda_1 & \\ & & & \lambda_2 \end{pmatrix}$	$\lambda_1 \xrightarrow{a_1} \lambda_2$	$p^k \phi(p^{k-i})$	$p^{6i} \phi(p^k) \mathrm{GL}_3(\mathbb{Z}_{p^k}) $
$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_1 & & \\ & & \lambda_2 & \\ & & & \lambda_2 \end{pmatrix}$	$\lambda_1 \xrightarrow{a_1} \lambda_2$	$\frac{p^k \phi(p^{k-i})}{2}$	$p^{8i} \mathrm{GL}_2(\mathbb{Z}_{p^k}) ^2$

Table 1. 4×4 diagonal matrix types with at most two distinct diagonal entries.

type T	valuation graph	$t(T)$	$c(T)$
$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_1 & & \\ & & \lambda_2 & \\ & & & \lambda_3 \end{pmatrix}$	$\lambda_1 \xrightarrow{a_1} \lambda_2 \xrightarrow{a_1} \lambda_3$	$\frac{p^k \phi(p^{k-i}) \phi_2(p^{k-i})}{2}$	$p^{10i} \phi(p^k)^2 \mathrm{GL}_2(\mathbb{Z}_{p^k}) $
$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_1 & & \\ & & \lambda_2 & \\ & & & \lambda_3 \end{pmatrix}$	$\lambda_1 \xrightarrow{a_1} \lambda_2 \xrightarrow{a_2} \lambda_3$	$\frac{3 p^k \phi(p^{k-i}) \phi(p^{k-j})}{2}$	$p^{6i+4j} \phi(p^k)^2 \mathrm{GL}_2(\mathbb{Z}_{p^k}) $
$\begin{pmatrix} \lambda_1 & & & \\ & \lambda_1 & & \\ & & \lambda_2 & \\ & & & \lambda_3 \end{pmatrix}$	$\lambda_1 \xrightarrow{a_1} \lambda_2 \xrightarrow{a_2} \lambda_3$	$\frac{3 p^k \phi(p^{k-i}) \phi(p^{k-j})}{2}$	$p^{8i+2j} \phi(p^k)^2 \mathrm{GL}_2(\mathbb{Z}_{p^k}) $

Table 2. 4×4 diagonal matrix types with three distinct diagonal entries.

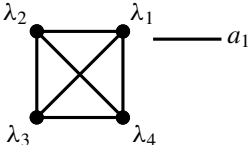
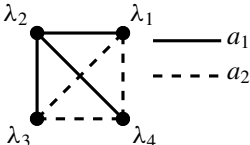
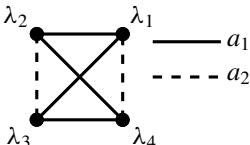
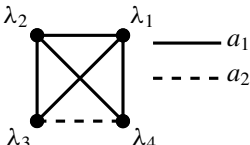
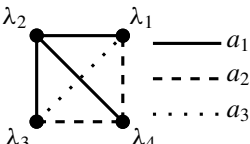
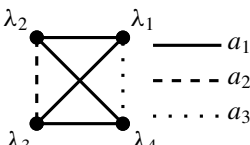
valuation graph	$t(T)$	$c(T)$
	$\frac{p^k \phi(p^{k-i}) \phi_2(p^{k-i}) \phi_3(p^{k-i})}{4!}$	$p^{12i} \phi(p^k)^4$
	$\binom{4}{3} \frac{p^k \phi(p^{k-i}) \phi(p^{k-j}) \phi_2(p^{k-j})}{4!}$	$p^{6i+6j} \phi(p^k)^4$
	$\frac{1}{2} \binom{4}{2} \frac{p^k \phi(p^{k-i}) \phi(p^{k-j})^2}{4!}$	$p^{8i+4j} \phi(p^k)^4$
	$\binom{4}{2} \frac{p^k \phi(p^{k-i}) \phi_2(p^{k-i}) \phi(p^{k-j})}{4!}$	$p^{10i+2j} \phi(p^k)^4$
	$\binom{4}{3} \binom{3}{1} \frac{p^k \phi(p^{k-i}) \phi(p^{k-j}) \phi(p^{k-m})}{4!}$	$p^{6i+4j+2m} \phi(p^k)^4$
	$\binom{4}{4} \binom{4}{2} \frac{p^k \phi(p^{k-i}) \phi(p^{k-j}) \phi(p^{k-m})}{4!}$	$p^{8i+2j+2m} \phi(p^k)^4$

Table 3. 4×4 diagonal matrix types with distinct diagonal entries.

It remains to enumerate the diagonal matrix types where the diagonal entries are distinct. By inspection, we find that there are six distinct classes of valuation graphs if we disregard the actual weights of their edges. We summarize the pertinent information for each of these six valuation graphs in Table 3.

By using (2), one can now find the number of 4×4 diagonalizable matrices over \mathbb{Z}_{p^k} . In light of the many cases from the three tables above, the final formula will be quite long and messy to explicitly write out, and we therefore have chosen not to include it here (although the curious reader should have no problem constructing it if necessary).

8. The proportion of diagonalizable matrices over \mathbb{Z}_{p^k}

Kaylor and Offner [2014] noted that as the size of the field \mathbb{F}_q increases, the proportion of matrices in $M_n(\mathbb{F}_q)$ with all eigenvalues in \mathbb{F}_q approaches $1/n!$; that is,

$$\lim_{q \rightarrow \infty} \frac{|\text{Eig}_n(\mathbb{F}_q)|}{|M_n(\mathbb{F}_q)|} = \frac{1}{n!}.$$

In particular, [Kaylor and Offner 2014] also implies that as the size of \mathbb{F}_q increases, the proportion of matrices in $M_n(\mathbb{F}_q)$ that are diagonalizable over \mathbb{F}_q approaches $1/n!$ as well. We generalize this latter result by replacing \mathbb{F}_q in the case of $q = p$ with \mathbb{Z}_{p^k} .

Theorem 8.1. *Fix positive integers n and k , and let p be a prime number. Then,*

$$\lim_{p \rightarrow \infty} \frac{|\text{Diag}_n(\mathbb{Z}_{p^k})|}{|M_n(\mathbb{Z}_{p^k})|} = \frac{1}{n!}.$$

Proof. Letting i index the distinct types of diagonal matrices, we let $T_{n,i}$ denote the i -th distinct type of a diagonal matrix in $M_n(\mathbb{Z}_{p^k})$. Note that we can view $|\text{Diag}_n(\mathbb{Z}_{p^k})|$ as a polynomial in powers of p . Since we are taking a limit as $p \rightarrow \infty$, it suffices to determine which diagonal matrix types contributes to the leading term of $|\text{Diag}_n(\mathbb{Z}_{p^k})|$. We accomplish this by first computing its degree:

$$\begin{aligned} \deg |\text{Diag}_n(\mathbb{Z}_{p^k})| &= \deg \left(\sum_{i=1}^{|\mathcal{T}(n)|} t(T_{n,i}) s(T_{n,i}) \right) \\ &= \max_{1 \leq i \leq |\mathcal{T}(n)|} \deg(t(T_{n,i}) s(T_{n,i})) \\ &= \max_{1 \leq i \leq |\mathcal{T}(n)|} \deg \left(t(T_{n,i}) \frac{|\text{GL}_n(\mathbb{Z}_{p^k})|}{c(T_{n,i})} \right) \\ &= \max_{1 \leq i \leq |\mathcal{T}(n)|} (\deg |\text{GL}_n(\mathbb{Z}_{p^k})| + \deg t(T_{n,i}) - \deg c(T_{n,i})) \\ &= \max_{1 \leq i \leq |\mathcal{T}(n)|} (kn^2 + \deg t(T_{n,i}) - \deg c(T_{n,i})). \end{aligned}$$

By Proposition 3.4, we find that

$$\begin{aligned} \deg c(T_{u,i}) &= \sum_{i=1}^r \deg |\text{GL}_{m_i}(\mathbb{Z}_{p^k})| + \sum_{1 \leq i < j \leq k} \deg p^{2m_i m_j l_{ij}} \\ &= k \sum_{i=1}^r m_i^2 + \sum_{1 \leq i < j \leq k} 2m_i m_j l_{ij} \\ &\geq k \sum_{i=1}^r m_i^2 && (\text{since each } l_{ij} \geq 0) \\ &\geq kn && (\text{since each } m_i \geq 1). \end{aligned}$$

Moreover, Theorem 5.7 yields

$$\deg t(T_{n,i}) = k + \sum_{t=1}^r \sum_{j=1}^{J_t} \sum_{i=1}^{|L_j^{(a_t)}|} (k - a_t) \leq k + \sum_{t=1}^r \sum_{j=1}^{J_t} k |L_j^{(a_t)}| = k + k(n-1) = kn.$$

Therefore $\deg t(T_{n,i}) \leq \deg c(T_{n,i})$, with equality occurring if and only if the diagonal matrix is of the type in which its diagonal entries are distinct and their differences are units in \mathbb{Z}_{p^k} . Hence, $\deg |\text{Diag}_n(\mathbb{Z}_{p^k})| = kn^2$, and using the aforementioned diagonal matrix type, the leading coefficient of $|\text{Diag}_n(\mathbb{Z}_{p^k})|$ equals $1/n!$ by Theorem 5.7. Thus, we have

$$\frac{|\text{Diag}_n(\mathbb{Z}_{p^k})|}{|M_n(\mathbb{Z}_{p^k})|} = \frac{(1/n!)p^{kn^2} + O(p^{kn^2-1})}{p^{kn^2}}.$$

The desired limit immediately follows by letting $p \rightarrow \infty$. \square

9. Future research

As we have seen, given a ring of the form \mathbb{Z}_{p^k} and a positive integer n , we have given a procedure to compute $|\text{Diag}_n(\mathbb{Z}_{p^k})|$. The main difficulty that remains is enumerating the possible valuation graph classes (up to automorphism and disregarding the actual values of the weights) corresponding to $n \times n$ diagonal matrices. As demonstrated in the previous sections, it suffices to enumerate such classes corresponding to $n \times n$ diagonal matrices with distinct diagonal entries; let a_n denote this quantity. We have seen that $a_2 = 3$ and $a_4 = 6$, and it turns out that $a_5 = 20$ (see Figure 4 for these classes). It would be of interest to find at least a recursive formula that determines a_n for a given value of n .

In addition to this, it would be of interest to extend our work to include matrices with Jordan canonical forms (JCFs) over \mathbb{Z}_{p^k} , that is, matrices similar to a block diagonal matrix comprised of the Jordan matrices

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

for some $\lambda \in \mathbb{Z}_{p^k}$. One would have to be careful performing such an enumeration, because it is possible for a given matrix to have more than one distinct JCF over \mathbb{Z}_{p^k} . For instance in \mathbb{Z}_4 , we have

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

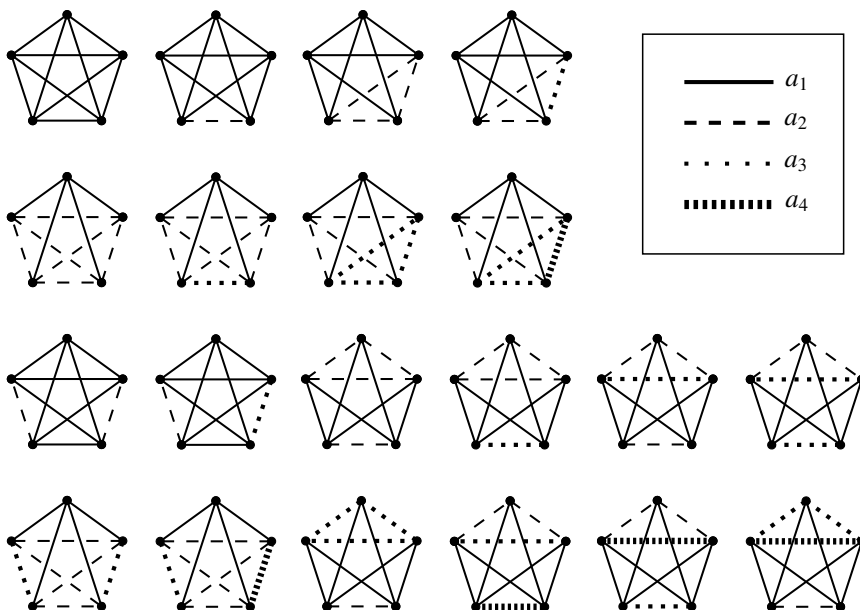


Figure 4. The twenty 5×5 valuation graph classes.

Although finding an enumeration formula for the centralizer of a Jordan matrix should be straightforward, this is not expected to be the case for an arbitrarily chosen JCF.

As a final remark, besides the potential nonuniqueness of a JCF, there is a reason why we have not enumerated $|\text{Eig}_n(\mathbb{Z}_{p^k})|$. Unlike in the finite-field case where any matrix in $\text{Eig}_n(\mathbb{F}_q)$ has a JCF (see [Kaylor and Offner 2014] for more details), this is not even necessarily the case in $\text{Eig}_n(\mathbb{Z}_{p^k})$. For example in \mathbb{Z}_{p^2} , any matrix of the form $\begin{pmatrix} \lambda & p \\ 0 & \lambda \end{pmatrix}$ has double eigenvalue λ , but lacks a Jordan canonical form over \mathbb{Z}_{p^2} . Determining all similarity classes of such matrices is in general still an open question.

References

- [Bollman and Ramírez 1969] D. Bollman and H. Ramírez, “On the enumeration of matrices over finite commutative rings”, *Amer. Math. Monthly* **76** (1969), 1019–1023. MR Zbl
- [Brown 1993] W. C. Brown, *Matrices over commutative rings*, Monographs and Textbooks in Pure and Applied Mathematics **169**, Marcel Dekker, New York, 1993. MR Zbl
- [Han 2006] J. Han, “The general linear group over a ring”, *Bull. Korean Math. Soc.* **43**:3 (2006), 619–626. MR Zbl
- [Kaylor and Offner 2014] L. Kaylor and D. Offner, “Counting matrices over a finite field with all eigenvalues in the field”, *Involve* **7**:5 (2014), 627–645. MR Zbl
- [Olšavský 2003] G. Olšavský, “The number of 2 by 2 matrices over $\mathbb{Z}/p\mathbb{Z}$ with eigenvalues in the same field”, *Math. Mag.* **76**:4 (2003), 314–317. MR Zbl

Received: 2019-08-12 Revised: 2019-11-27 Accepted: 2019-12-23

c.falvey24@gmail.com *American University, Washington, D.C., United States*

heewonhah@gmail.com *University of North Carolina, Charlotte, NC, United States*

sheppard@math.ucsb.edu *University of California, Santa Barbara, CA, United States*

bdsittinger@gmail.com *California State University Channel Islands, Camarillo, CA, United States*

ricoevicente@gmail.com *California State University, Long Beach, CA, United States*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

MANAGING EDITOR

Kenneth S. Berenhaut Wake Forest University, USA

BOARD OF EDITORS

Colin Adams	Williams College, USA	Robert B. Lund	Clemson University, USA
Arthur T. Benjamin	Harvey Mudd College, USA	Gaven J. Martin	Massey University, New Zealand
Martin Bohner	Missouri U of Science and Technology, USA	Mary Meyer	Colorado State University, USA
Amarjit S. Budhiraja	U of N Carolina, Chapel Hill, USA	Frank Morgan	Williams College, USA
Pietro Cerone	La Trobe University, Australia	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran
Scott Chapman	Sam Houston State University, USA	Zuhair Nashed	University of Central Florida, USA
Joshua N. Cooper	University of South Carolina, USA	Ken Ono	Univ. of Virginia, Charlottesville
Jem N. Corcoran	University of Colorado, USA	Yuval Peres	Microsoft Research, USA
Toka Diagana	University of Alabama in Huntsville, USA	Y.-F. S. Pétermann	Université de Genève, Switzerland
Michael Dorff	Brigham Young University, USA	Jonathon Peterson	Purdue University, USA
Sever S. Dragomir	Victoria University, Australia	Robert J. Plemmons	Wake Forest University, USA
Joel Foisy	SUNY Potsdam, USA	Carl B. Pomerance	Dartmouth College, USA
Errin W. Fulp	Wake Forest University, USA	Vadim Ponomarenko	San Diego State University, USA
Joseph Gallian	University of Minnesota Duluth, USA	Bjorn Poonen	UC Berkeley, USA
Stephan R. Garcia	Pomona College, USA	József H. Przytycki	George Washington University, USA
Anant Godbole	East Tennessee State University, USA	Richard Rebarber	University of Nebraska, USA
Ron Gould	Emory University, USA	Robert W. Robinson	University of Georgia, USA
Sat Gupta	U of North Carolina, Greensboro, USA	Javier Rojo	Oregon State University, USA
Jim Haglund	University of Pennsylvania, USA	Filip Saidak	U of North Carolina, Greensboro, USA
Johnny Henderson	Baylor University, USA	Hari Mohan Srivastava	University of Victoria, Canada
Glenn H. Hurlbert	Virginia Commonwealth University, USA	Andrew J. Sterge	Honorary Editor
Charles R. Johnson	College of William and Mary, USA	Ann Trenk	Wellesley College, USA
K. B. Kulasekera	Clemson University, USA	Ravi Vakil	Stanford University, USA
Gerry Ladas	University of Rhode Island, USA	Antonia Vecchio	Consiglio Nazionale delle Ricerche, Italy
David Larson	Texas A&M University, USA	John C. Wierman	Johns Hopkins University, USA
Suzanne Lenhart	University of Tennessee, USA	Michael E. Zieve	University of Michigan, USA
Chi-Kwong Li	College of William and Mary, USA		

PRODUCTION

Silvio Levy, Scientific Editor


Cover: Alex Scorpan

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2020 is US \$205/year for the electronic version, and \$275/year (+\$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1444-4184 electronic, 1444-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2020 Mathematical Sciences Publishers

involve

2020

vol. 13

no. 2

Arithmetic functions of higher-order primes	181
KYLE CZARNECKI AND ANDREW GIDDINGS	
Spherical half-designs of high order	193
DANIEL HUGHES AND SHAYNE WALDRON	
A series of series topologies on \mathbb{N}	205
JASON DEVITO AND ZACHARY PARKER	
Discrete Morse functions, vector fields, and homological sequences on trees	219
IAN RAND AND NICHOLAS A. SCOVILLE	
An explicit third-order one-step method for autonomous scalar initial value problems of first order based on quadratic Taylor approximation	231
THOMAS KRAINER AND CHENZHANG ZHOU	
New generalized secret-sharing schemes with points on a hyperplane using a Wronskian matrix	257
WESTON LOUCKS AND BAHATTIN YILDIZ	
Generalized Cantor functions: random function iteration	281
JORDAN ARMSTRONG AND LISBETH SCHAUBROECK	
Numerical semigroup tree of multiplicities 4 and 5	301
ABBY GRECO, JESSE LANSFORD AND MICHAEL STEWARD	
Enumerating diagonalizable matrices over \mathbb{Z}_{p^k}	323
CATHERINE FALVEY, HEEWON HAH, WILLIAM SHEPPARD, BRIAN SITTINGER AND RICO VICENTE	
On arithmetical structures on complete graphs	345
ZACHARY HARRIS AND JOEL LOUWSMA	
Connectedness of digraphs from quadratic polynomials	357
SIJI CHEN AND SHENG CHEN	

