Matrices modulo p^k and k commuting matrices modulo p

Amritanshu Prasad

24 April 2015

Similarity and simultaneous similarity

Definition of Similarity

Similarity and simultaneous similarity

Definition of Similarity

Matrices A and B in $M_n(R)$ are similar if there exists $X \in GL_n(R)$ such that

$$XAX^{-1} = B.$$

Similarity and simultaneous similarity

Definition of Similarity

Matrices A and B in $M_n(R)$ are similar if there exists $X \in GL_n(R)$ such that

$$XAX^{-1} = B.$$

Here R can be any ring.

Simultaneous Similarity

Similarity and simultaneous similarity

Definition of Similarity

Matrices A and B in $M_n(R)$ are similar if there exists $X \in GL_n(R)$ such that

$$XAX^{-1} = B.$$

Here R can be any ring.

Simultaneous Similarity

The tuple $(A_1, \ldots, A_k)$ is similar to the tuple $(B_1, \ldots, B_k)$ if there exists $X \in GL_n(R)$ such that

$$XA_1X^{-1} = B_1, XA_2X^{-1} = B_2, \cdots, XA_kX^{-1} = B_k.$$

Classes in a Field

Rational Canonical Form

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

where $f_k | f_{k-1} | \ldots | f_1$.

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

where $f_k | f_{k-1} | \ldots | f_1$.
Here C_f is the companion matrix of f.

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

where $f_k | f_{k-1} | \ldots | f_1$.
Here C_f is the companion matrix of f.

In a finite field

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

where $f_k | f_{k-1} | \ldots | f_1$.
Here C_f is the companion matrix of f.

In a finite field

Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ be a partition of n.

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

where $f_k | f_{k-1} | \ldots | f_1$.
Here C_f is the companion matrix of f.

In a finite field

Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ be a partition of n.
Number of classes with $\deg(f_i) = \lambda_i$ is

$$q^{\lambda_k + (\lambda_{k-1} - \lambda_k) + \cdots (\lambda_2 - \lambda_1)} = q^{\lambda_1}$$

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

where $f_k | f_{k-1} | \ldots | f_1$.
Here C_f is the companion matrix of f.

In a finite field

Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ be a partition of n.
Number of classes with $\deg(f_i) = \lambda_i$ is

$$q^{\lambda_k + (\lambda_{k-1} - \lambda_k) + \cdots (\lambda_2 - \lambda_1)} = q^{\lambda_1}$$

Why?

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

where $f_k | f_{k-1} | \ldots | f_1$.
Here C_f is the companion matrix of f.

In a finite field

Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ be a partition of n.
Number of classes with $\deg(f_i) = \lambda_i$ is

$$q^{\lambda_k + (\lambda_{k-1} - \lambda_k) + \cdots (\lambda_2 - \lambda_1)} = q^{\lambda_1}$$

Why?
$f_1, \ldots, f_k$ is determined by $f_1/f_2, f_2/f_3, \ldots, f_{k-1}/f_k, f_k$.

Classes in a Field

Rational Canonical Form

$$A \sim C_{f_1} \oplus C_{f_2} \oplus \cdots \oplus C_{f_k}$$

where $f_k | f_{k-1} | \ldots | f_1$.
Here C_f is the companion matrix of f.

In a finite field

Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ be a partition of n.
Number of classes with $\deg(f_i) = \lambda_i$ is

$$q^{\lambda_k + (\lambda_{k-1} - \lambda_k) + \cdots (\lambda_2 - \lambda_1)} = q^{\lambda_1}$$

Why?
$f_1, \ldots, f_k$ is determined by $f_1/f_2, f_2/f_3, \ldots, f_{k-1}/f_k, f_k$.
No. of choices for $f_i/f_{i+1} = q^{\lambda_i - \lambda_{i+1}}$.

Matrix tuple problem

Matrix tuple problem

$$a_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Matrix tuple problem

$$a_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Burnside's Lemma:

Matrix tuple problem

$$a_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Burnside's Lemma:

$$a_{n,k}(q) = \frac{1}{|GL_n(\mathbf{F}_q)|} \sum_{g \in GL_n(\mathbf{F}_q)} |Z_{M_n(\mathbf{F}_q)}(g)|^k.$$

Matrix tuple problem

$$a_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Burnside's Lemma:

$$a_{n,k}(q) = \frac{1}{|GL_n(\mathbf{F}_q)|} \sum_{g \in GL_n(\mathbf{F}_q)} |Z_{M_n(\mathbf{F}_q)}(g)|^k.$$

Shows that

Matrix tuple problem

$$a_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Burnside's Lemma:

$$a_{n,k}(q) = \frac{1}{|GL_n(\mathbf{F}_q)|} \sum_{g \in GL_n(\mathbf{F}_q)} |Z_{M_n(\mathbf{F}_q)}(g)|^k.$$

Shows that

$$A_n(q,t) = \sum_{k=0}^{\infty} a_{n,k}(q) t^k = \frac{1}{|GL_n(\mathbf{F}_q)|} \sum_{g \in GL_n(\mathbf{F}_q)} \frac{1}{1 - |Z_{M_n(\mathbf{F}_q)}(g)|t},$$

Matrix tuple problem

$$a_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Burnside's Lemma:

$$a_{n,k}(q) = \frac{1}{|GL_n(\mathbf{F}_q)|} \sum_{g \in GL_n(\mathbf{F}_q)} |Z_{M_n(\mathbf{F}_q)}(g)|^k.$$

Shows that

$$A_n(q,t) = \sum_{k=0}^{\infty} a_{n,k}(q) t^k = \frac{1}{|GL_n(\mathbf{F}_q)|} \sum_{g \in GL_n(\mathbf{F}_q)} \frac{1}{1 - |Z_{M_n(\mathbf{F}_q)}(g)|t},$$

is a rational function of t for each n.

Theory of Types

Theory of Types

Jordan normal form

Theory of Types

Jordan normal form

Similarity classes in $M_n(\mathbf{F}_q)$ correspond to

$$\{\phi : \mathrm{Irr}\mathbf{F}_q[t] \to \Lambda \mid \sum_{f \in \mathrm{Irr}\mathbf{F}_q[t]} \deg(f)|\phi(f)| = n\}$$

Theory of Types

Jordan normal form

Similarity classes in $M_n(\mathbf{F}_q)$ correspond to

$$\{\phi : \mathrm{Irr}\mathbf{F}_q[t] \to \Lambda \mid \sum_{f \in \mathrm{Irr}\mathbf{F}_q[t]} \deg(f)|\phi(f)| = n\}$$

Types

Theory of Types

Jordan normal form

Similarity classes in $M_n(\mathbf{F}_q)$ correspond to

$$\{\phi : \mathrm{Irr}\mathbf{F}_q[t] \to \Lambda \mid \sum_{f \in \mathrm{Irr}\mathbf{F}_q[t]} \deg(f)|\phi(f)| = n\}$$

Types

Classes ϕ_1 and ϕ_2 have the same type if

Theory of Types

Jordan normal form

Similarity classes in $M_n(\mathbf{F}_q)$ correspond to

$$\{\phi : \mathrm{Irr}\mathbf{F}_q[t] \to \Lambda \mid \sum_{f \in \mathrm{Irr}\mathbf{F}_q[t]} \deg(f)|\phi(f)| = n\}$$

Types

Classes ϕ_1 and ϕ_2 have the same type if

$$\phi_2 = \phi_2 \circ \sigma$$

Theory of Types

Jordan normal form

Similarity classes in $M_n(\mathbf{F}_q)$ correspond to

$$\{\phi : \mathrm{Irr}\mathbf{F}_q[t] \to \Lambda \mid \sum_{f \in \mathrm{Irr}\mathbf{F}_q[t]} \deg(f)|\phi(f)| = n\}$$

Types

Classes ϕ_1 and ϕ_2 have the same type if

$$\phi_2 = \phi_2 \circ \sigma$$

for some degree-preserving bijection $\sigma : \mathrm{Irr}\mathbf{F}_q[t] \to \mathrm{Irr}\mathbf{F}_q[t]$.

Why types are useful

Why types are useful

Types are combinatorial

Why types are useful

Types are combinatorial

- Given ϕ, define $\tau : \Lambda \to \Lambda$ by

$$\tau_\phi(\lambda) = (1^{m_1}, 2^{m_2}, \dots)$$

where m_i is the number of irreducible polynomials f of degree i such that $\phi(i) = \lambda$. Then ϕ_1 and ϕ_2 have the same type if and only if $\tau_{\phi_1} = \tau_{\phi_2}$.

Why types are useful

Types are combinatorial

- Given ϕ, define $\tau : \Lambda \to \Lambda$ by

$$\tau_\phi(\lambda) = (1^{m_1}, 2^{m_2}, \dots)$$

where m_i is the number of irreducible polynomials f of degree i such that $\phi(i) = \lambda$. Then ϕ_1 and ϕ_2 have the same type if and only if $\tau_{\phi_1} = \tau_{\phi_2}$.

- The set of types is a combinatorial object; types correspond to functions

$$\{\tau : \Lambda \to \Lambda \mid \sum_{\lambda \in \Lambda} |\lambda||\tau(\lambda)| = n\}$$

Why types are useful

Types are combinatorial

- Given ϕ, define $\tau : \Lambda \to \Lambda$ by

$$\tau_\phi(\lambda) = (1^{m_1}, 2^{m_2}, \dots)$$

where m_i is the number of irreducible polynomials f of degree i such that $\phi(i) = \lambda$. Then ϕ_1 and ϕ_2 have the same type if and only if $\tau_{\phi_1} = \tau_{\phi_2}$.

- The set of types is a combinatorial object; types correspond to functions

$$\{\tau : \Lambda \to \Lambda \mid \sum_{\lambda \in \Lambda} |\lambda||\tau(\lambda)| = n\}$$

- The number of matrices of each type can be counted

Why types are useful

Types are combinatorial

- Given ϕ, define $\tau : \Lambda \to \Lambda$ by

$$\tau_\phi(\lambda) = (1^{m_1}, 2^{m_2}, \dots)$$

where m_i is the number of irreducible polynomials f of degree i such that $\phi(i) = \lambda$. Then ϕ_1 and ϕ_2 have the same type if and only if $\tau_{\phi_1} = \tau_{\phi_2}$.

- The set of types is a combinatorial object; types correspond to functions

$$\{\tau : \Lambda \to \Lambda \mid \sum_{\lambda \in \Lambda} |\lambda||\tau(\lambda)| = n\}$$

- The number of matrices of each type can be counted

- Matrices of the same type have isomorphic centralizers

Computer Implementation

```
sage: from sage.combinat.similarity_class_type import *
sage: q = ZZ['q'].gen()
sage: def simultaneous_similarity_classes(n,k):
....:     return SimilarityClassTypes(n).sum(lambda la: q**(
sage: simultaneous_similarity_classes(3, 2)
q^10 + q^8 + 2*q^7 + 2*q^6 + 2*q^5 + q^4
```

Kac conjecture

Kac conjecture

- Usually stated in the framework of quivers

Kac conjecture

- Usually stated in the framework of quivers
- When the quiver has one vertex and k loops (bouquet quiver) isomorphism classes of representations are simultaneous similarity classes of matrices

Kac conjecture

- Usually stated in the framework of quivers
- When the quiver has one vertex and k loops (bouquet quiver) isomorphism classes of representations are simultaneous similarity classes of matrices

Conjecture (V. Kac, 1983)

Kac conjecture

- Usually stated in the framework of quivers
- When the quiver has one vertex and k loops (bouquet quiver) isomorphism classes of representations are simultaneous similarity classes of matrices

Conjecture (V. Kac, 1983)

$a_{n,k}(q)$ is a polynomial in q with non-negative integer coefficients

Kac conjecture

- Usually stated in the framework of quivers
- When the quiver has one vertex and k loops (bouquet quiver) isomorphism classes of representations are simultaneous similarity classes of matrices

Conjecture (V. Kac, 1983)

$a_{n,k}(q)$ is a polynomial in q with non-negative integer coefficients
This result was proved by Hausel, Letellier and Rodriguez-Villegas, 2013.

Commuting Matrix Tuple Problem

Commuting Matrix Tuple Problem

$$b_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of commuting } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Commuting Matrix Tuple Problem

$$b_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of commuting } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Generating function

Commuting Matrix Tuple Problem

$$b_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of commuting } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Generating function

$$B_n(q,t) = \sum_{k=0}^{\infty} b_{n,k}(q) t^k$$

Commuting Matrix Tuple Problem

$$b_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of commuting } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Generating function

$$B_n(q,t) = \sum_{k=0}^{\infty} b_{n,k}(q) t^k$$

This is a rational function.

Commuting Matrix Tuple Problem

$$b_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of commuting } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Generating function

$$B_n(q,t) = \sum_{k=0}^{\infty} b_{n,k}(q) t^k$$

This is a rational function.

Not known

Commuting Matrix Tuple Problem

$$b_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of commuting } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Generating function

$$B_n(q,t) = \sum_{k=0}^{\infty} b_{n,k}(q) t^k$$

This is a rational function.

Not known

Are its coefficients polynomials in q?

Commuting Matrix Tuple Problem

$$b_{n,k}(q) = \begin{array}{l}\text{No. of simultaneous similarity classes of} \\ k\text{-tuples of commuting } n \times n \text{ matrices over } \mathbf{F}_q.\end{array}$$

Generating function

$$B_n(q,t) = \sum_{k=0}^{\infty} b_{n,k}(q) t^k$$

This is a rational function.

Not known

Are its coefficients polynomials in q?

Explicit Computation (Uday Bhaskar Sharma)

n	$B_n(q,t)$
1	$\frac{1}{1-qt}$
2	$\frac{1}{(1-qt)(1-q^2t)}$
3	$\frac{1+q^2t^2}{(1-qt)(1-q^2t)(1-q^3t)}$
4	$\left(\frac{1+q^2t+2q^2t^2+q^3t^2+2q^4t^2+q^6t^3}{(1-qt)(1-q^2t)(1-q^3t)(1-q^4t)(1-q^5t)}\right)$ $-\left(\frac{q^5t+q^7t^2+q^3t^3+2q^7t^3+2q^9t^3+q^{10}t^4}{(1-qt)(1-q^2t)(1-q^3t)(1-q^4t)(1-q^5t)}\right)$

Explicit Computation (Uday Bhaskar Sharma)

n	$B_n(q,t)$
1	$\frac{1}{1-qt}$
2	$\frac{1}{(1-qt)(1-q^2t)}$
3	$\frac{1+q^2t^2}{(1-qt)(1-q^2t)(1-q^3t)}$
4	$\left(\frac{1+q^2t+2q^2t^2+q^3t^2+2q^4t^2+q^6t^3}{(1-qt)(1-q^2t)(1-q^3t)(1-q^4t)(1-q^5t)}\right)$ $-\left(\frac{q^5t+q^7t^2+q^3t^3+2q^7t^3+2q^9t^3+q^{10}t^4}{(1-qt)(1-q^2t)(1-q^3t)(1-q^4t)(1-q^5t)}\right)$

Conclusion

Explicit Computation (Uday Bhaskar Sharma)

n	$B_n(q,t)$
1	$\frac{1}{1-qt}$
2	$\frac{1}{(1-qt)(1-q^2t)}$
3	$\frac{1+q^2t^2}{(1-qt)(1-q^2t)(1-q^3t)}$
4	$\left(\frac{1+q^2t+2q^2t^2+q^3t^2+2q^4t^2+q^6t^3}{(1-qt)(1-q^2t)(1-q^3t)(1-q^4t)(1-q^5t)}\right)$ $-\left(\frac{q^5t+q^7t^2+q^3t^3+2q^7t^3+2q^9t^3+q^{10}t^4}{(1-qt)(1-q^2t)(1-q^3t)(1-q^4t)(1-q^5t)}\right)$

Conclusion

$b_{n,k}(q)$ is a polynomial in q with non-negative integer coefficients for $n \leq 4$.

Similarity classes modulo p^k

Similarity classes modulo p^k

$$c_{n,k}(q) = \text{No. of similarity classes of } n \times n \text{ matrices in } M_n(\mathbf{Z}/p^k\mathbf{Z}).$$

Similarity classes modulo p^k

$c_{n,k}(q) =$ No. of similarity classes of $n \times n$ matrices in $M_n(\mathbf{Z}/p^k\mathbf{Z})$.

Generating Function

Similarity classes modulo p^k

$c_{n,k}(q) =$ No. of similarity classes of $n \times n$ matrices in $M_n(\mathbf{Z}/p^k\mathbf{Z})$.

Generating Function

$$C_n(q,t) = \sum_{k=0}^{\infty} c_{n,k}(q)t^k$$

Similarity classes modulo p^k

$c_{n,k}(q) =$ No. of similarity classes of $n \times n$ matrices in $M_n(\mathbf{Z}/p^k\mathbf{Z})$.

Generating Function

$$C_n(q,t) = \sum_{k=0}^{\infty} c_{n,k}(q)t^k$$

is known to be a rational function of t.

Similarity classes modulo p^k

$c_{n,k}(q) =$ No. of similarity classes of $n \times n$ matrices in $M_n(\mathbf{Z}/p^k\mathbf{Z})$.

Generating Function

$$C_n(q,t) = \sum_{k=0}^{\infty} c_{n,k}(q)t^k$$

is known to be a rational function of t.

Calculations for $k = 2$ (Prasad, Singla and Spallone)

n	$c_{n,2}(q)$
2	$q^4 + q^3 + q^2$
3	$q^6 + q^5 + 2q^4 + q^3 + 2q^2$
4	$q^8 + q^7 + 3q^6 + 3q^5 + 5q^4 + 3q^3 + 3q^2$

Relation to simultaneous similarity classes

Relation to simultaneous similarity classes

Theorem

$$b_{n,2}(p) = c_{n,2}(p).$$

See Singla, Jambor and Plesken and also: Prasad, Singla and Spallone, Remark 1.1

Outline of Proof

Outline of Proof

Theorem (Main Lemma)

For every $A \in M_n(\mathbf{Z}/p\mathbf{Z})$, *there exists* $\tilde{A} in M_n(\mathbf{Z}/p^2\mathbf{Z})$ *such that for every* $B \in M_n(\mathbf{Z}/p\mathbf{Z})$ *that commutes with* A *there exists* $\tilde{B} in M_n(\mathbf{Z}/p^2\mathbf{Z})$ *that commutes with* $\tilde{A}$.

A reduction

A reduction

Let $A \in M_n(\mathbf{Z}/p\mathbf{Z})$.

A reduction

Let $A \in M_n(\mathbf{Z}/p\mathbf{Z})$. Define

$$G_A = \{\tilde{X} \in GL_n(\mathbf{Z}/p^2\mathbf{Z}) \mid \tilde{X}\tilde{A} \cong \tilde{A}\tilde{X} \mod p\}.$$

A reduction

Let $A \in M_n(\mathbf{Z}/p\mathbf{Z})$. Define

$$G_A = \{\tilde{X} \in GL_n(\mathbf{Z}/p^2\mathbf{Z}) \mid \tilde{X}\tilde{A} \cong \tilde{A}\tilde{X} \mod p\}.$$

The map:

$$C \mapsto C \cap \tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$$

A reduction

Let $A \in M_n(\mathbf{Z}/p\mathbf{Z})$. Define

$$G_A = \{\tilde{X} \in GL_n(\mathbf{Z}/p^2\mathbf{Z}) \mid \tilde{X}\tilde{A} \cong \tilde{A}\tilde{X} \mod p\}.$$

The map:

$$C \mapsto C \cap \tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$$

defines a bijection from the set of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which which contain a lift of A to the set of G_A-orbits in $\tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$.

A reduction

Let $A \in M_n(\mathbf{Z}/p\mathbf{Z})$. Define

$$G_A = \{\tilde{X} \in GL_n(\mathbf{Z}/p^2\mathbf{Z}) \mid \tilde{X}\tilde{A} \cong \tilde{A}\tilde{X} \mod p\}.$$

The map:

$$C \mapsto C \cap \tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$$

defines a bijection from the set of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which which contain a lift of A to the set of G_A-orbits in $\tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$.
So, in order to classify similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$, it suffices to

A reduction

Let $A \in M_n(\mathbf{Z}/p\mathbf{Z})$. Define

$$G_A = \{\tilde{X} \in GL_n(\mathbf{Z}/p^2\mathbf{Z}) \mid \tilde{X}\tilde{A} \cong \tilde{A}\tilde{X} \mod p\}.$$

The map:

$$C \mapsto C \cap \tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$$

defines a bijection from the set of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which which contain a lift of A to the set of G_A-orbits in $\tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$.
So, in order to classify similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$, it suffices to

- classify similarity classes in $M_n(\mathbf{Z}/p\mathbf{Z})$ (which has been done)

A reduction

Let $A \in M_n(\mathbf{Z}/p\mathbf{Z})$. Define

$$G_A = \{\tilde{X} \in GL_n(\mathbf{Z}/p^2\mathbf{Z}) \mid \tilde{X}\tilde{A} \cong \tilde{A}\tilde{X} \mod p\}.$$

The map:

$$C \mapsto C \cap \tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$$

defines a bijection from the set of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which which contain a lift of A to the set of G_A-orbits in $\tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$.
So, in order to classify similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$, it suffices to

- classify similarity classes in $M_n(\mathbf{Z}/p\mathbf{Z})$ (which has been done)
- for some A in each such class, find G_A-orbits in $\tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$

A lemma on group actions

A lemma on group actions

The lemma

Let G be a group acting on a set X, and let N be a normal subgroup of G.

A lemma on group actions

The lemma

Let G be a group acting on a set X, and let N be a normal subgroup of G. Then G/N has a well-defined action on $N\backslash X$, and

A lemma on group actions

The lemma

Let G be a group acting on a set X, and let N be a normal subgroup of G. Then G/N has a well-defined action on $N\backslash X$, and

$$G\backslash X = (G/N)\backslash(N\backslash X).$$

A lemma on group actions

The lemma

Let G be a group acting on a set X, and let N be a normal subgroup of G. Then G/N has a well-defined action on $N\backslash X$, and

$$G\backslash X = (G/N)\backslash(N\backslash X).$$

In our case

A lemma on group actions

The lemma

Let G be a group acting on a set X, and let N be a normal subgroup of G. Then G/N has a well-defined action on $N\backslash X$, and

$$G\backslash X = (G/N)\backslash(N\backslash X).$$

In our case

$G = G_A$, $X = \tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$.

A lemma on group actions

The lemma

Let G be a group acting on a set X, and let N be a normal subgroup of G. Then G/N has a well-defined action on $N\backslash X$, and

$$G\backslash X = (G/N)\backslash(N\backslash X).$$

In our case

$G = G_A$, $X = \tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$.
$N = \{I + pX \mid X \in M_n(\mathbf{Z}/p\mathbf{Z})$.

A lemma on group actions

The lemma

Let G be a group acting on a set X, and let N be a normal subgroup of G. Then G/N has a well-defined action on $N\backslash X$, and

$$G\backslash X = (G/N)\backslash(N\backslash X).$$

In our case

$G = G_A$, $X = \tilde{A} + pM_n(\mathbf{Z}/p\mathbf{Z})$.
$N = \{I + pX \mid X \in M_n(\mathbf{Z}/p\mathbf{Z})$.
G/N is isomorphic to $Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}A$.

N-orbits in X

N-orbits in X

$\tilde{A} + pX$ and $\tilde{A} + pY$ are in the same N orbit if and only if there exists $U \in M_n(\mathbf{Z}/p\mathbf{Z})$ such that

N-orbits in X

$\tilde{A} + pX$ and $\tilde{A} + pY$ are in the same N orbit if and only if there exists $U \in M_n(\mathbf{Z}/p\mathbf{Z})$ such that

$$(I + pU)(\tilde{A} + pX) = (\tilde{A} + pY)(I + pU).$$

N-orbits in X

$\tilde{A} + pX$ and $\tilde{A} + pY$ are in the same N orbit if and only if there exists $U \in M_n(\mathbf{Z}/p\mathbf{Z})$ such that

$$(I + pU)(\tilde{A} + pX) = (\tilde{A} + pY)(I + pU).$$

Equivalently

N-orbits in X

$\tilde{A} + pX$ and $\tilde{A} + pY$ are in the same N orbit if and only if there exists $U \in M_n(\mathbf{Z}/p\mathbf{Z})$ such that

$$(I + pU)(\tilde{A} + pX) = (\tilde{A} + pY)(I + pU).$$

Equivalently

$$X - Y \in [A, M_n(\mathbf{Z}/p\mathbf{Z})].$$

N-orbits in X

$\tilde{A} + pX$ and $\tilde{A} + pY$ are in the same N orbit if and only if there exists $U \in M_n(\mathbf{Z}/p\mathbf{Z})$ such that

$$(I + pU)(\tilde{A} + pX) = (\tilde{A} + pY)(I + pU).$$

Equivalently

$$X - Y \in [A, M_n(\mathbf{Z}/p\mathbf{Z})].$$

So:

$$N\backslash X = M_n(\mathbf{Z}/p\mathbf{Z})/[A, M_n(\mathbf{Z}/p\mathbf{Z})]$$

Duality

Duality

Identify $M_n(\mathbf{Z}/p\mathbf{Z})$ with its linear dual using the non-degenerate bilinear form

$$\langle X, Y \rangle = \mathrm{trace}(XY).$$

Duality

Identify $M_n(\mathbf{Z}/p\mathbf{Z})$ with its linear dual using the non-degenerate bilinear form

$$\langle X, Y \rangle = \mathrm{trace}(XY).$$

This form is invariant under the action of $GL_n(\mathbf{Z}/p\mathbf{Z})$, and so also the action of $G/N = Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)$.

Duality

Identify $M_n(\mathbf{Z}/p\mathbf{Z})$ with its linear dual using the non-degenerate bilinear form

$$\langle X, Y \rangle = \mathrm{trace}(XY).$$

This form is invariant under the action of $GL_n(\mathbf{Z}/p\mathbf{Z})$, and so also the action of $G/N = Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)$.
This gives rise to an isomorphism

Duality

Identify $M_n(\mathbf{Z}/p\mathbf{Z})$ with its linear dual using the non-degenerate bilinear form

$$\langle X, Y \rangle = \mathrm{trace}(XY).$$

This form is invariant under the action of $GL_n(\mathbf{Z}/p\mathbf{Z})$, and so also the action of $G/N = Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)$.
This gives rise to an isomorphism

$$\left(\frac{M_n(\mathbf{Z}/p\mathbf{Z})}{[A, M_n(\mathbf{Z}/p\mathbf{Z})]} \right)^* = Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)$$

Duality

Identify $M_n(\mathbf{Z}/p\mathbf{Z})$ with its linear dual using the non-degenerate bilinear form

$$\langle X, Y \rangle = \mathrm{trace}(XY).$$

This form is invariant under the action of $GL_n(\mathbf{Z}/p\mathbf{Z})$, and so also the action of $G/N = Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)$.
This gives rise to an isomorphism

$$\left(\frac{M_n(\mathbf{Z}/p\mathbf{Z})}{[A, M_n(\mathbf{Z}/p\mathbf{Z})]} \right)^* = Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)$$

which preserves the action of $Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)$.

Group actions on vector spaces and their duals

Group actions on vector spaces and their duals

Let X be a finite vector space, and G be a finite group acting by linear maps.

Group actions on vector spaces and their duals

Let X be a finite vector space, and G be a finite group acting by linear maps. Then

$$|G\backslash X| = |G\backslash X^*|$$

Group actions on vector spaces and their duals

Let X be a finite vector space, and G be a finite group acting by linear maps. Then

$$|G\backslash X| = |G\backslash X^*|$$

This follows from Burnside's lemma:

Group actions on vector spaces and their duals

Let X be a finite vector space, and G be a finite group acting by linear maps. Then

$$|G\backslash X| = |G\backslash X^*|$$

This follows from Burnside's lemma:

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

Group actions on vector spaces and their duals

Let X be a finite vector space, and G be a finite group acting by linear maps. Then

$$|G\backslash X| = |G\backslash X^*|$$

This follows from Burnside's lemma:

$$|G\backslash X| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

Now note that X^g is the 1-eigenspace of g, which has the same dimension as the 1-eigenspace of g^*.

Finishing the proof

Finishing the proof

So the number of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which contain an element congruent to $A \mod p$ is

Finishing the proof

So the number of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which contain an element congruent to $A \mod p$ is

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash\Big(M_n(\mathbf{Z}/p\mathbf{Z})/[A, M_n(\mathbf{Z}/p\mathbf{Z})]\Big)$$

Finishing the proof

So the number of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which contain an element congruent to $A \mod p$ is

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash\Big(M_n(\mathbf{Z}/p\mathbf{Z})/[A, M_n(\mathbf{Z}/p\mathbf{Z})]\Big)$$

which is the same as

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)$$

Finishing the proof

So the number of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which contain an element congruent to $A \mod p$ is

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash\Big(M_n(\mathbf{Z}/p\mathbf{Z})/[A, M_n(\mathbf{Z}/p\mathbf{Z})]\Big)$$

which is the same as

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)$$

So the number $c_{n,k}(p)$ of similarity classes in $M_n(\mathbf{Z}/p^{\mathbf{Z}})$ is

Finishing the proof

So the number of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which contain an element congruent to $A \mod p$ is

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash\Big(M_n(\mathbf{Z}/p\mathbf{Z})/[A, M_n(\mathbf{Z}/p\mathbf{Z})]\Big)$$

which is the same as

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)$$

So the number $c_{n,k}(p)$ of similarity classes in $M_n(\mathbf{Z}/p^{\mathbf{Z}})$ is

$$\sum_A |Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)|$$

Finishing the proof

So the number of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which contain an element congruent to $A \mod p$ is

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash\Big(M_n(\mathbf{Z}/p\mathbf{Z})/[A, M_n(\mathbf{Z}/p\mathbf{Z})]\Big)$$

which is the same as

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)$$

So the number $c_{n,k}(p)$ of similarity classes in $M_n(\mathbf{Z}/p^{\mathbf{Z}})$ is

$$\sum_A |Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)|$$

the sum being over all similarity classes in $M_n(\mathbf{Z}/p\mathbf{Z})$.

Finishing the proof

So the number of similarity classes in $M_n(\mathbf{Z}/p^2\mathbf{Z})$ which contain an element congruent to $A \mod p$ is

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash\Big(M_n(\mathbf{Z}/p\mathbf{Z})/[A, M_n(\mathbf{Z}/p\mathbf{Z})]\Big)$$

which is the same as

$$Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)$$

So the number $c_{n,k}(p)$ of similarity classes in $M_n(\mathbf{Z}/p^{\mathbf{Z}})$ is

$$\sum_A |Z_{GL_n(\mathbf{Z}/p\mathbf{Z})}(A)\backslash Z_{M_n(\mathbf{Z}/p\mathbf{Z})}(A)|$$

the sum being over all similarity classes in $M_n(\mathbf{Z}/p\mathbf{Z})$.
This is $b_{n,k}(p)$.

Conjectures

Conjectures

- $B_n(p,t) = C_n(p,t)$ for all n.

Conjectures

- $B_n(p,t) = C_n(p,t)$ for all n. This is known for $n \leq 3$, by work of Avni, Onn, Prasad and Vaserstein

Conjectures

- $B_n(p,t) = C_n(p,t)$ for all n. This is known for $n \leq 3$, by work of Avni, Onn, Prasad and Vaserstein
- these are polynomials in p with non-negative integer coefficients.