

MATHEMATICS 402

GUEST LECTURE

OCTOBER 28, 2016

JAYADEV ATHREYA

---

# FINITE MATRIX GROUPS

## 2 X 2 MATRICES

- ▶ Let  $a, b, c, d$  be real numbers
- ▶ When does  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  have a (multiplicative) inverse?
- ▶ Can we form a group out of  $2 \times 2$  matrices with matrix multiplication?

## 2 X 2 MATRICES

- ▶ Let  $a, b, c, d$  be in  $\mathbb{Z}_p$ , the integers mod  $p$ .
- ▶ When does  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  have a (multiplicative) inverse? What is it?
- ▶ Can we form a group out of  $2 \times 2$  matrices with matrix multiplication?

## GENERAL LINEAR GROUP OVER $\mathbb{Z}_p$

- ▶ Let  $a, b, c, d$  be in  $\mathbb{Z}_p$ , the integers mod  $p$ .
- ▶ The set of matrices  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  with  $ad-bc \neq 0$  is called  $GL(2, p)$ .
- ▶  $GL(2, p)$  is a group under matrix multiplication.
- ▶ How many elements are there?

## GENERAL LINEAR GROUP OVER $\mathbb{Z}_p$

- ▶ Let  $a, b, c, d$  be in  $\mathbb{Z}_p$ , the integers mod  $p$ .
- ▶ The set of matrices  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  with  $ad-bc \neq 0$  is called  $GL(2, p)$ .
- ▶  $GL(2, p)$  is a group under matrix multiplication.
- ▶ How many elements are there?
  - ▶ What can the first column be?
  - ▶ What can the second column be?
  - ▶ Can we generalize to  $GL(n, p)$ ?

**GL(N, P) CONTAINS**  
 **$(P^N - 1)(P^N - P)(P^N - P^2) \dots$**   
 **$\dots (P^N - P^{N-2})(P^N - P^{N-1})$**   
**ELEMENTS**

**GENERAL LINEAR GROUP MOD P**