0.1 Week 1, Discussion 1

Problem. Fix a prime p. How many invertible $n \times n$ matrices are there over $\mathbb{F}_p$? In other words, find $|\mathrm{GL}_n(\mathbb{F}_p)|$.

Solution. We use the elementary fact from linear algebra that a matrix is invertible if and only if its rows are linearly independent. We proceed by a counting argument.

Suppose $A \in \mathbb{F}_p^{n \times n}$ is invertible. How many possibilities are there for the first row of A? We need the rows to form an independent set, so the first row can be anything but the zero vector, which gives $p^n - 1$ possible first rows (p^n row vectors in total, minus the one "bad" vector).

How many possible second rows? Whatever the second row is, it must be independent of the first row, so it can be anything but a multiple of the first row. There are p possible multiples of the first row since we're working in $\mathbb{F}_p$, so there are $p^n - p$ possible second rows.

How many possible k-th rows? The k-th row can be anything but a linear combination of the $k-1$ rows that came before it. A linear combination of the rows $v_1, \dots v_{k-1}$ looks like

$$c_1 v_1 + c_2 v_2 + \cdots + c_{k-1} v_{k-1},$$

where the c_i's come from $\mathbb{F}_p$. There are $k-1$ constants to choose, each of which can take any value in $\mathbb{F}_p$, so there are p^{k-1} linear combinations in total. We want to get rid of these, so there are $p^n - p^{k-1}$ possible k-th rows.

Now we put it all together.

$$\begin{aligned} |\mathrm{GL}_n(\mathbb{F}_p)| &= \#\{\text{possible first rows}\} \cdots \#\{\text{possible } n\text{-th rows}\} \\ &= (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) \\ &= \prod_{j=0}^{n-1} (p^n - p^j). \end{aligned}$$

From here you answer other questions like how big is $\mathrm{SL}_n(\mathbb{F}_p)$, the set of $n \times n$ matrices with determinant 1. Consider the map $\det : \mathrm{GL}_n(\mathbb{F}_p) \to \mathbb{F}_p^\times$. Since the determinant is multiplicative, the map det is a group homomorphism. By the first isomorphism theorem, $\mathrm{GL}_n(\mathbb{F}_p)/\ker\det \cong \mathbb{F}_p^\times$. The kernel of det is the set of matrices that get sent to 1, which is exactly $\mathrm{SL}_n(\mathbb{F}_p)$. We then have $|\mathrm{GL}_n(\mathbb{F}_p)|/|\mathrm{SL}_n(\mathbb{F}_p)| = |\mathbb{F}_p^\times| = p - 1$. Rearranging gives

$$|\mathrm{SL}_n(\mathbb{F}_p)| = \frac{1}{p-1} |\mathrm{GL}_n(\mathbb{F}_p)|.$$

□