

Homework 14

Recall that the set of keys for a Hill ciphers of size m on an n -letter alphabet is

$$GL_m(\mathbf{Z}_n) = \{A \in Mat_{m \times m}(\mathbf{Z}_n) \mid \det(A) \in \mathbf{Z}_n^*\}$$

where $Mat_{m \times m}(\mathbf{Z}_n)$ is the set of all m by m matrices with entries in \mathbf{Z}_n .

Suppose p is a prime. Prove that

$$|GL_m(\mathbf{Z}_p)| = (p^m - 1)(p^m - p)(p^m - p^2) \cdots (p^m - p^{m-1})$$

(Hint: You may take as known that linear algebra works as usual over \mathbf{Z}_p when p is prime. In particular, $\det(A) \in \mathbf{Z}_p^* \iff \det(a) \not\equiv 0 \pmod{p} \iff$ the rows of A are linearly independent over \mathbf{Z}_p . Count how many choices there are for the first row, and given that, how many choices are left for the second row, and so on.)