

## Homework 12

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 prime and  $n, m \in \mathbf{Z}^+$ .

a) Consider the function

$$f: Mat_{m \times m}(\mathbf{Z}_{p^n}) \rightarrow Mat_{m \times m}(\mathbf{Z}_p)$$

given by  $f(A) = A \bmod p$ . Prove

$$A \in GL_m(\mathbf{Z}_{p^n}) \iff f(A) \in GL_m(\mathbf{Z}_p).$$

b) Prove that for each  $B \in GL_m(\mathbf{Z}_p)$ , there there are  $p^{(n-1)m^2}$  matrices  $A \in GL_m(\mathbf{Z}_{p^n})$  with  $f(A) = B$ .

Note, this proves that

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