

## Homework 13

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  $r, s \in \mathbf{Z}^+$  with  $\gcd(r, s) = 1$ .

- a) Prove that if  $a \in \mathbf{Z}$ ,  $\gcd(a, rs) = 1$  iff  $\gcd(a, r) = 1$  and  $\gcd(a, s) = 1$ .
- b) Consider the function

$$f: Mat_{m \times m}(\mathbf{Z}_{rs}) \rightarrow Mat_{m \times m}(\mathbf{Z}_r) \times Mat_{m \times m}(\mathbf{Z}_s)$$

given by  $f(A) = (A \bmod r, A \bmod s)$ . Prove that  $f$  is a bijection.

- c) Prove that  $f(GL_m(\mathbf{Z}_{rs})) = GL_m(\mathbf{Z}_r) \times GL_m(\mathbf{Z}_s)$ .

Note, this proves that

$$|GL_m(\mathbf{Z}_{rs})| = |GL_m(\mathbf{Z}_r)| \cdot |GL_m(\mathbf{Z}_s)|$$