

1. For positive integers  $m, n$ , we'll be using the following (standard) notation.

$$\begin{aligned} \text{Mat}_m(\mathbb{Z}/n\mathbb{Z}) &= \{m \times m \text{ matrices with entries that are integers mod } n\} \\ \text{GL}_m(\mathbb{Z}/n\mathbb{Z}) &= \{A \in \text{Mat}_m(\mathbb{Z}/n\mathbb{Z}) : A \text{ is invertible mod } n\}. \end{aligned}$$

Let  $p$  be a prime and let  $k, m$  be positive integers. Define a function

$$f : \text{Mat}_m(\mathbb{Z}/p^k\mathbb{Z}) \rightarrow \text{Mat}_m(\mathbb{Z}/p\mathbb{Z}) \quad \text{by setting} \quad f(A) := A \pmod{p},$$

i.e., reduce each entry of  $A$  modulo  $p$ .

- Show:  $A \in \text{GL}_m(\mathbb{Z}/p^k\mathbb{Z})$  if and only if  $f(A) \in \text{GL}_m(\mathbb{Z}/p\mathbb{Z})$ .
- Show: For each  $B \in \text{GL}_m(\mathbb{Z}/p\mathbb{Z})$ , there are  $p^{m^2(k-1)}$  matrices  $A \in \text{GL}_m(\mathbb{Z}/p^k\mathbb{Z})$  that satisfy  $f(A) = B$ .
- Use part b to show that  $|\text{GL}_m(\mathbb{Z}/p^k\mathbb{Z})| = p^{m^2(k-1)}|\text{GL}_m(\mathbb{Z}/p\mathbb{Z})|$  (where, for any set  $X$ , the notation  $|X|$  denotes the cardinality of  $X$ ).

2. Let  $a, b$  be positive integers, and suppose  $\gcd(a, b) = 1$ .

- Show (for any  $x \in \mathbb{Z}$ ) that  $\gcd(x, ab) = 1$  if and only if  $\gcd(x, a) = 1$  and  $\gcd(x, b) = 1$ .
- Define a function

$$\begin{aligned} h : \text{Mat}_m(\mathbb{Z}/ab\mathbb{Z}) &\rightarrow \text{Mat}_m(\mathbb{Z}/a\mathbb{Z}) \times \text{Mat}_m(\mathbb{Z}/b\mathbb{Z}) \\ &\text{by setting} \quad h(A) := (A \pmod{a}, A \pmod{b}). \end{aligned}$$

Show that  $h$  is bijective.

- Now consider the image (under  $h$ ) of the invertible matrices, and show:  $h(\text{GL}_m(\mathbb{Z}/ab\mathbb{Z})) = \text{GL}_m(\mathbb{Z}/a\mathbb{Z}) \times \text{GL}_m(\mathbb{Z}/b\mathbb{Z})$ .
- Use part c to show that  $|\text{GL}_m(\mathbb{Z}/ab\mathbb{Z})| = |\text{GL}_m(\mathbb{Z}/a\mathbb{Z})| \cdot |\text{GL}_m(\mathbb{Z}/b\mathbb{Z})|$ .

3. Let  $p$  be a prime. Show that  $|\text{GL}_m(\mathbb{Z}/p\mathbb{Z})| = (p^m - 1)(p^m - p)(p^m - p^2) \cdots (p^m - p^{m-1})$ . You can do this by looking at an arbitrary  $A \in \text{GL}_m(\mathbb{Z}/p\mathbb{Z})$  and counting how many ways there are to create the first row of  $A$ ; once you have the first row, how many ways are there to create the second row of  $A$ ? (Remember  $A$  has to be invertible, so its rows must be linearly independent!) Continue counting row by row to obtain the given expression.

4. Suppose you know your adversary is using a certain cipher whose key is a  $3 \times 3$  matrix modulo 26, and you want to attack their ciphertext message by exhaustive search. At worst how many different keys would you have to test? What if the key is  $4 \times 4$ ?  $m \times m$ ?

5. Let  $n > 1$  be an integer and let  $\varphi$  denote Euler's totient function.

- What is the relationship between  $\text{GL}_1(\mathbb{Z}/n\mathbb{Z})$  and  $\varphi(n)$ ?
- Use your results from questions 1 – 3 to show the following: If  $p_1, p_2, \dots, p_t$  are distinct primes and  $e_1, e_2, \dots, e_t$  are positive integers, then

$$\varphi(p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}) = p_1^{e_1-1} (p_1 - 1) p_2^{e_2-1} (p_2 - 1) \cdots p_t^{e_t-1} (p_t - 1).$$