

**1:** Find the Smith Normal Form of the following matrices

(a)

$$\begin{pmatrix} 4 & 2 & -1 \\ 3 & 1 & 0 \\ 0 & 7 & 2 \end{pmatrix}$$

(b)

$$\begin{pmatrix} 7 & 0 \\ 0 & 2 \end{pmatrix}$$

via operations on columns and rows that are invertible on  $\mathbb{Z}^{n \times n}$ . You should track the operations you perform and collect them in two matrices  $U, V \in GL_n(\mathbb{Z})$  such that  $UAV = D$ , where  $D \in \mathbb{Z}^{n \times n}$  is a diagonal matrix, whose entries on the diagonal  $d_1, \dots, d_n$  are such that  $d_1 | d_2 | \dots | d_n$ .

This form is unique up to multiplication with  $\pm 1$ . Moreover, one can show that

$$d_1 \cdots d_i = g.c.d\{A_j \mid A_j \text{ is an } i \times i \text{ submatrix of } A, \forall j\}$$

**Remark:** a slightly weaker factorization is just as useful for solving binomial systems: just reduce to a diagonal matrix (and neglect the divisibility condition). You lose uniqueness, but the resulting normal form is equally useful for solving the system (and quicker to get!).

**2:**

(a) Find all the third-powers in  $\mathbb{F}_{27}$ .

(b) How many solutions does  $x^4 = 6$  have in  $\mathbb{F}_{17}$ ?

**Remark:** Recall exercise 5 of hw1:

$$x^d = c \text{ has a root in } \mathbb{F}_q \Leftrightarrow c^{\frac{q-1}{gcd(q-1, d)}} = 1 \text{ in } \mathbb{F}_q \quad q = p^k$$