Smith normal form let A be any square matrix over a pid R. then there exist a sequence of invertible row and column operations on A transforming it into the form $\operatorname{diag}(d_1, \ldots, d_r, 0, \ldots, 0)$ where $d_1 \mid \ldots \mid d_r$.

algorithm over Euclidean domains

1. if $A = 0$ terminate.

otherwise, find $a_{ij} \neq 0$ and perform $R_1 \leftrightarrow R_j$ & $C_1 \leftrightarrow C_j$.

2. once $a_{11} \neq 0$, if there is an element a_{1j} of the first row or an element a_{i1} of the first column not divisible by a_{11}, decrease the norm of a_{11} via $(\star)$ and return to step 2.

3. once a_{11} divides all elements in the first row and column, make A into $\begin{pmatrix} a_{11} & 0 & \cdots \\ 0 & * & * \\ \vdots & * & * \end{pmatrix}$ via $(\star\star)$.

4. if a_{11} does not divide all the elements of A, decrease the norm of a_{11} via $(\star\star\star)$ and return to step 2.

5. once a_{11} divides all elements of A, apply the algorithm for the reduced, lower right part of A.

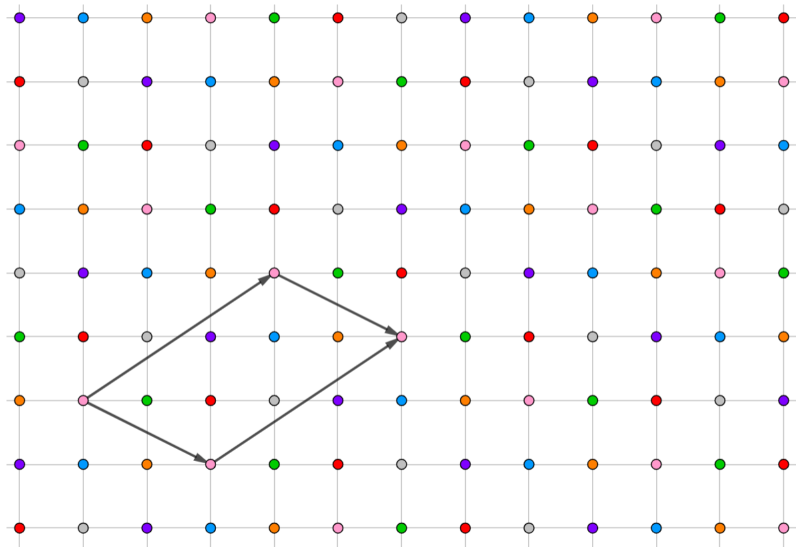
exercise find the steps $(\star), (\star\star)$ and $(\star\star\star)$ and prove the algorithm's correctness.

exercise

i. let $A \in \mathbf{Z}^{d\times d}$ have determinant ± 1. then A^{-1} has integer entries.

ii. more generally, let $v_1, \ldots, v_d \in \mathbf{Z}^d$ be linearly independent over $\mathbf{R}$. then

$$[\mathbf{Z}^d : \mathbf{Z}v_1 \oplus \ldots \oplus \mathbf{Z}v_d] = |[0,1)v_1 + \ldots + [0,1)v_n \cap \mathbf{Z}^n| = |\det v_{ij}|$$



$$7 = \det \begin{pmatrix} 2 & 3 \\ -1 & 2 \end{pmatrix} = [\mathbf{Z}^2 : \mathbf{Z} \begin{bmatrix} 2 \\ -1 \end{bmatrix} \oplus \mathbf{Z} \begin{bmatrix} 3 \\ 2 \end{bmatrix}]$$