The Smith normal form theorem says the following:

**Theorem (Smith normal form).** Let \( R \) be a principal ideal domain and let \( X \) be an \( m \times n \) matrix with entries in \( R \). Then there invertible \( m \times m \) and \( n \times n \) matrices \( U \) and \( V \), and elements \( d_1, d_2, \ldots, d_{\min(m,n)} \) of \( R \), such that
\[
X = UDV,
\]
where \( D \) is the \( m \times n \) matrix with \( D_{ij} = d_j \) and \( D_{ij} = 0 \) for \( i \neq j \). Moreover, we may assume \( d_1|d_2|\cdots|d_{\min(m,n)} \) and, with this normalization, the \( d_j \) are unique up to multiplication by units.

The \( d_j \) are called the **invariant factors** of \( X \). We first set up some notation:

(92) Let \( R \) be any ring. Define an relation \( \sim \) on \( \text{Mat}_{m\times n}(R) \) by \( X \sim Y \) if there are invertible \( m \times m \) and \( n \times n \) matrices \( U \) and \( V \) with \( Y = UXV \). Show that \( \sim \) is an equivalence relation. \(^2\)

(93) Here is a more abstract perspective on \( \sim \): Let \( X \) and \( Y \in \text{Mat}_{m\times n}(R) \).

(a) Show that \( X \sim Y \) if and only if we can choose vertical isomorphisms making the following diagram commute:
\[
\begin{array}{ccc}
R^n & \xrightarrow{X} & R^n \\
\downarrow \cong & & \downarrow \cong \\
R^n & \xleftarrow{Y} & R^n \\
\end{array}
\]
(b) Show that, if \( X \sim Y \), then the kernels, cokernels and images of \( X \) and \( Y \) are isomorphic \( R \)-modules. \(^3\)

For nonnegative integers \( m \) and \( n \), and elements \( d_1, d_2, \ldots, d_{\min(m,n)} \) of \( R \), we define \( \text{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)}) \) to be the \( m \times n \) matrix \( D \) above. Thus, Smith normal form says that every matrix is \( \sim \)-equivalent to a matrix of the form \( \text{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)}) \) with \( d_1|d_2|\cdots|d_{\min(m,n)} \) and the \( d_j \) are unique up to multiplication by units.

It will be convenient today to know the following formula. The morally right proof of this result will be more natural in a month, so you may assume it for now.

**The Cauchy-Binet formula.** Let \( R \) be a commutative ring. Given an \( m \times n \) matrix \( X \) with entries in \( R \), and subsets \( I \subseteq \{1, 2, \ldots, m \} \) and \( J \subseteq \{1, 2, \ldots, n \} \) of the same size, define \( \Delta_{IK}(X) \) to be the determinant of the square submatrix of \( X \) using rows \( I \) and columns \( J \). Let \( X \) and \( Y \) be \( a \times b \) and \( b \times c \) matrices with entries in \( R \) and let \( I \) and \( K \) be subsets of \( \{1, 2, \ldots, a \} \) and \( \{1, 2, \ldots, c \} \) with \(|I| = |J| = q \). Then
\[
\Delta_{IK}(XY) = \sum_{J \subseteq \{1, 2, \ldots, b \}, \quad |J| = q} \Delta_{IJ}(X)\Delta_{JK}(Y).
\]

The next few problems show how to compute invariant factors.

(94) Let \( R \) be a UFD. Let \( U, X \) and \( V \) be \( m \times m, m \times n \) and \( n \times n \) matrices with entries in \( R \). Show that the GCD of the \( q \times q \) minors of \( X \) divides the GCD of the \( q \times q \) minors of \( UXV \).

(95) Let \( R \) be a UFD. Show that, if \( X \sim Y \), then the GCD of the \( q \times q \) minors of \( X \) is equal to the GCD of the \( q \times q \) minors of \( Y \).

(96) Let \( R \) be a UFD. Let \( X \) be an \( m \times n \) matrix with entries in \( R \). Show that, if \( X \sim \text{diag}_{mn}(d_1, d_2, \ldots, d_{\min(m,n)}) \) with \( d_1|d_2|\cdots|d_{\min(m,n)} \), then \( d_1d_2\cdots d_q \) is the GCD of the \( q \times q \) minors of \( X \). Deduce that invariant factors are uniquely defined up to multiplication by units.

(97) Assuming the Smith normal form theorem for \( \mathbb{Z} \), compute the invariant factors of the following matrices:
\[
\begin{bmatrix}
2 & 0 \\
0 & 3
\end{bmatrix}, \quad \begin{bmatrix}
2 & 1 \\
0 & 2
\end{bmatrix}, \quad \begin{bmatrix}
2 & -1 & -1 \\
-1 & 2 & -1 \\
-1 & -1 & 2
\end{bmatrix}.
\]

(98) If you have gotten this far, go ahead and prove the Cauchy-Binet formula. It can be done by brute force.

---

\(^1\) Named for Henry John Stephen Smith, an Irish mathematician who lived from 1826 to 1883.

\(^2\) The factorization \( UDV \) may remind the reader of singular value decomposition. This is not a coincidence; Smith normal form can be thought of as a non-Archimedean version of singular value decomposition.

\(^3\) The converse does not hold, see https://mathoverflow.net/questions/343143.