Práctica 2: Cifrado Afín y Cifrado Hill

1 Comenzamos definiendo las tres siguientes funciones:

- **algeucl:** Toma dos elementos y realiza el algoritmo de euclides. Devuelve el máximo común divisor entre los dos números. También verifica que los elementos introducidos son apropiados para la realización del algoritmo.
- **invmod:** Toma dos naturales p y n y calcula (si existe) el inverso de p en $\mathbb{Z}_n$. Avisa en caso de no existir.
- **eulerfun:** En este caso toma solo un natural n y devuelve un listado con todos los elementos invertibles en $\mathbb{Z}_n$.
- **InvModMatrix:** Toma una matriz A y un valor n y calcula (si existe) la inversa de A en

2 Definimos una función **TexttoNumber** que nos coge una cadena de caracteres y nos devuelve la correspondiente cadena numérica en $\mathbb{Z}_{26}$. Como en la práctica anterior, eliminamos espacios y signos especiales.

3 Sobre el cifrado afín:

- Programar el cifrado afín **Afincypher**: el programa debe tener como entrada el texto llano y dos valores k y d (recordamos que estamos considerando la transformación $f(x) = kx + d$). Se debe comprobar que los valores de k y d son válidos para el cifrado y devolver el texto cifrado.
- Programar el descifrado afín **Afindecypher**: Dado un texto cifrado y los anteriores k y d, devuelve el texto plano.
- Criptoanálisis: Finalmente, vamos a crear un programa para realizar el criptoanálisis de un texto cifrado y tratar de obtener el texto plano. Usaremos las funciones de la práctica anterior en relación al estudio de frecuencias. Programaremos las siguientes funciones:
  - Una función **guesskd** que debe tomar dos identificaciones de letras y nos devuelve los posibles k y d. Por identificaciones de letras se quiere decir identificaciones del tipo $p \to e$, donde p es la letra del texto cifrado y e es la supuesta letra en el texto llano. Esas dos identificaciones pueden darse como se prefiera (por ejemplo, con un diccionario $iden = 'q' :' e', 'r' =' a'$).
  - Una función **Afincriptoanalisis** interactiva que utilice todas las funciones anteriores para tratar de obtener el texto llano.

4 Sobre el cifrado Hill: Realizar un trabajo similar al hecho para el cifrado afín, pero con el cifrado Hill.