Criptografía: Aspectos Teóricos y Prácticos — Práctico 0

1. Implementar en `SAGE` el algoritmo extendido de Euclides visto en la clase práctica. Utilizarlo para hallar u y v tales que $au + bv = \gcd(a, b)$, donde $a = 16534528044$ y $b = 8332745927$.

2. Escriba las tablas de multiplicar de $\mathbb{Z}/10\mathbb{Z}$ y $\mathbb{Z}/11\mathbb{Z}$. ¿Qué diferencias observa?

3. Resolver las siguientes ecuaciones en $\mathbb{Z}/m\mathbb{Z}$.

   a) $3x + 4 \equiv 5 \mod 7$.
   b) $x^2 \equiv 3 \mod 11$.
   c) $x^2 \equiv 8 \mod 13$.
   d) $x^2 \equiv 1 \mod 8$.
   e) $x^2 + 10x + 10 \equiv 0 \mod 11$. Se puede usar la fórmula para hallar raíces de polinomios cuadráticos; pensar cómo.

4. Sea $m \in \mathbb{Z}$.

   a) Supongamos que m es impar. ¿Qué entero entre 1 y $m - 1$ es el inverso de 2 módulo m?
   b) Más generalmente, supongamos que $m \equiv 1 \mod b$. ¿Qué entero entre 1 y $m - 1$ es el inverso de b módulo m?

5. En cada uno de los siguientes casos, hallar el inverso de a módulo p de las siguientes dos maneras: (i) usando el algoritmo extendido de Euclides y (ii) usando el pequeño teorema de Fermat.

   a) $p = 7, a = 4$.
   b) $p = 31, a = 25$.

   Al utilizar el pequeño teorema de Fermat, hacerlo realizando la menor cantidad de multiplicaciones posible.

   Comentario: En el próximo práctico veremos una herramienta para calcular potencias rápidamente.

6. Resolver los siguientes sistemas de ecuaciones.

   a) $\begin{cases} x \equiv 4 \mod 5 \\ x \equiv 3 \mod 11 \end{cases}$

   b) $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 4 \mod 7 \end{cases}$

   En el primer ítem, hallar una solución en $\mathbb{Z}/55\mathbb{Z}$. En el segundo, en $\mathbb{Z}/105\mathbb{Z}$.

7. Explicar por qué el sistema de ecuaciones

$$\begin{cases} x \equiv 4 \mod 6 \\ x \equiv 5 \mod 15 \end{cases}$$

   no tiene solución.