

Implementar en SAGE los siguientes algoritmos.

**(1) Primos de la forma  $x^2 + y^2$ :**

**INPUT:**  $p$  primo.

**OUTPUT:** True,  $x, y$ ; si existen  $x, y \in \mathbb{Z}$  tal que  $p = x^2 + y^2$ . False en otro caso.

– Crear una lista con los primos menores a 1000. En el caso en el que sean suma de dos cuadrados especificar  $x$  e  $y$ .

– Conjeturar que cumplen dichos primos.

**(2) Congruencia Lineal:**

**INPUT:**  $a, b, m \in \mathbb{Z}$ ,  $m > 0$ .

**OUTPUT:** Soluciones  $x \in \mathbb{Z}/m\mathbb{Z}$  tal que  $ax \equiv b \pmod{m}$  en el caso en el que tenga solución. Congruencia Lineal sin solución en otro caso.

Ejemplos del uso de este algoritmo.

**(3) Teorema chino del resto:**

**INPUT:**  $m_1, b_1, \dots, m_r, b_r \in \mathbb{Z}$  tal que  $(m_i, m_j) = 1$  si  $i \neq j$ .

**OUTPUT:**  $x \in \mathbb{Z}/m\mathbb{Z}$  donde  $m = m_1 \cdots m_r$  tal que

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \dots\dots\dots \\ x \equiv b_r \pmod{m_r} \end{cases}$$

Ejemplos del uso de este algoritmo.

**(4) Congruencias mod  $m$ :**

**INPUT:**  $m \in \mathbb{N}$  y  $f(x, y) \in \mathbb{Z}[x, y]$ .

**OUTPUT:** Soluciones  $x, y \in \mathbb{Z}/m\mathbb{Z}$  tal que  $f(x, y) \equiv 0 \pmod{m}$ .

Ejemplos del uso de este algoritmo.

**(5) Lema de Hensel:**

**INPUT:**  $m \in \mathbb{N}$  y  $f(x, y) \in \mathbb{Z}[x, y]$ .

**OUTPUT:** Para cada primo  $p$  dividiendo a  $m$  utilizar el lema de Hensel para obtener soluciones  $x, y \in \mathbb{Z}/m\mathbb{Z}$  tal que  $f(x, y) \equiv 0 \pmod{m}$ .

Ejemplos del uso de este algoritmo.

**(6) Símbolo de Kronecker:**

**INPUT:**  $m, n \in \mathbb{Z}$ .

**OUTPUT:**  $\left(\frac{m}{n}\right)$ .

Ejemplos del uso de este algoritmo.

**Nota:** En todos los algoritmos anteriores se tendrá en cuenta para la calificación la velocidad del algoritmo.