

CURSO DE 8 HORAS ALGORITMOS DE PRIMALIDAD

1. LEY DE RECIPROCIDAD CUADRÁTICA. APLICACIONES: LOS TEST DE PRIMALIDAD CLÁSICOS (2 HORAS)

- La Ley de Reciprocidad Cuadrática (LRC).
- Aplicaciones: El Test de Proth. Números de Fermat y el Test de Pépin.
- El símbolo cuadrático y LRC en anillos de enteros de extensiones cuadráticas de \mathbb{Q} .
- Aplicaciones: El Test Lucasiano. El Test de Lucas Lehmer para Números de Mersenne.
- Números de Bosma.

2. LEYES DE RECIPROCIDAD CÚBICA Y BICUADRÁTICA. APLICACIONES A PRIMALIDAD

- Números de Mersenne cuadráticos y números de Fermat Cuadráticos.
- Casos particulares: Los Números de Mersenne Gaussianos y de Eisentein.
- Leyes de reciprocidad cúbica y bicuadrática.
- Aplicaciones:
 - (1) Test de Primalidad de los Números de Mersenne Gaussianos y de Eisentein.
 - (2) Primalidad de Números de Bosma.
- Problemas abiertos.

3. LEYES DE RECIPROCIDAD DE ORDEN SUPERIOR. ALGORITMOS APLICABLES A TODOS LOS ENTEROS. EL ALGORITMO APRCL Y EL ALGORITMO ECPP

- Primalidad en el siglo XX
- Leyes de Reciprocidad de orden superior.
- Aplicaciones: La generalización del Teorema de Proth.
- Combinando los test lucasianos y el de Proth: el test $n^2 - 1$.
- Algoritmos de Primalidad aplicables a cualquier entero: El algoritmo de ciclotomía.
- Algoritmos basados en la Teoría de Curvas Elípticas.

4. EL ALGORITMO AKS. PROBLEMAS DE INTERÉS EN EL ÁREA

- Primalidad en el siglo XXI: El algoritmo AKS.
- La versión práctica de AKS.
- El estado actual de AKS.
- Los problemas abiertos en el área.