1 Algoritmos obligatorios

1. Algoritmo de euclides para R un D.E cualquiera. y algoritmo de euclides extendido
2. Algoritmo para calcular el teorema chino del resto (i.e. calcular el inverso)
3. Mcd en un D.F.U.
4. Inverso de un elemento en un cuerpo finito. p,f irreducibles en $Zp[x] -> K := Zp[x]/(f(x))|K| = p^(degf)$
5. Test de irreducibilidad de un poliomio en Fq[x]
6. Logaritmo discreto en cuerpos Fq[x]/(f(x))
7. Algoritmo de factorización de un polinomio en cuerpo finito parte 1, 2 y 3
8. Algoritmo de factorización de Berlekamp en cuerpos finitos
9. Algoritmos de factorización en Z[x]
10. Algoritmo de primalidad de AKS

2 Algoritmos adicionales - Parte opcional

1. Algoritmo de Buchberger
2. Algoritmo de cuándo un elemento pertenece a un ideal
3. Algoritmo de división en varias variables - resto único
4. Algoritmo de primalidad de Miller-Rabin