Universidad Católica
San Pablo

INVESTIGACIÓN E IMPLEMENTACIÓN DE ALGORITMOS DE EXPONENCIACIÓN MODULAR

Integrantes:
Becerra Sipiran, Cledy Elizabeth
Oviedo Sivincha, Massiel
Villanueva Borda, Harold Alejandro

Docente:
Dc. Ana Maria Cuadros Valdivia

Curso:
Álgebra Abstracta

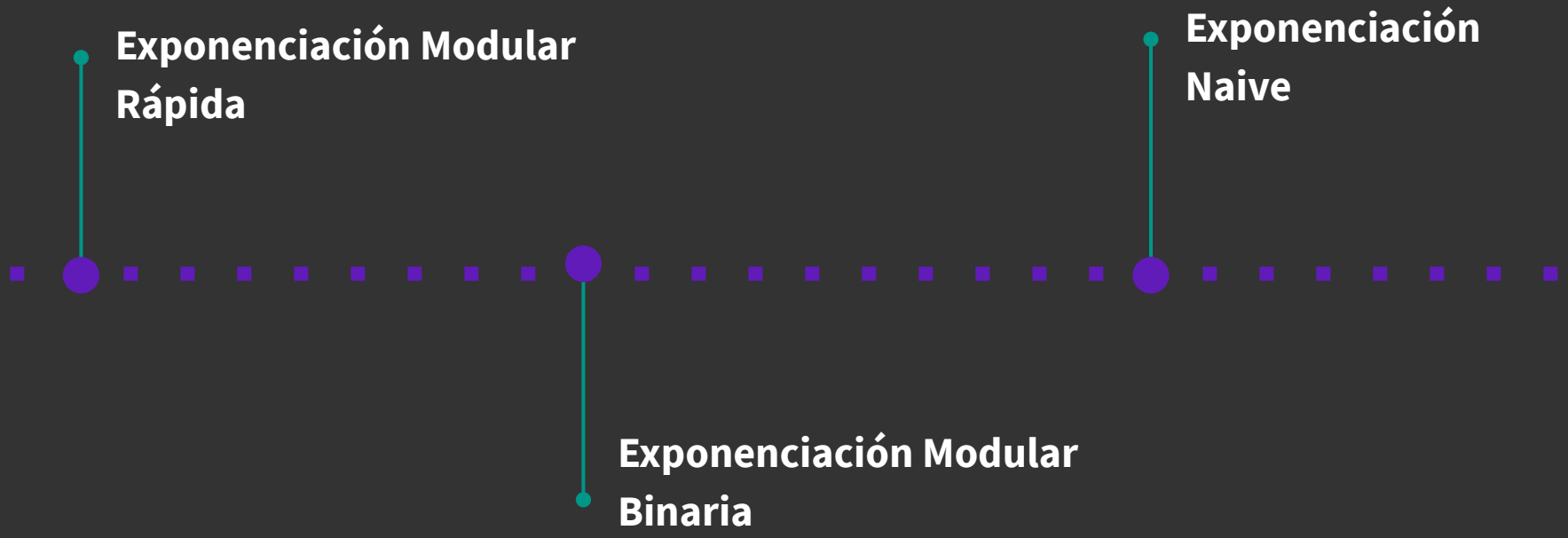
Departamento de Ciencia de la Computación
Universidad Católica San Pablo

Semestre 2021 - III
Arequipa - Perú

Introducción:

- Investigar las diversas variantes del Algoritmo de Exponenciación Modular.
- Analizar algoritmos y evaluar su eficiencia.
- Encontrar los algoritmos más eficientes entre los investigados.

Exponenciación Modular



El Mejor Algoritmo:

Exponenciación Modular Binaria

- Menor tiempo de ejecución
- Similitud con la exponenciación binaria left-right y right-left

Código:

IMPUT: a, n and m = (n−1 ...n0)
OUTPUT: The element a^n mod m.
1. r = 1
2. while n different from 0
   2.1 if n is odd then
      2.2.1 a = a^2 modulo m
   2.2 n/2
4 return r

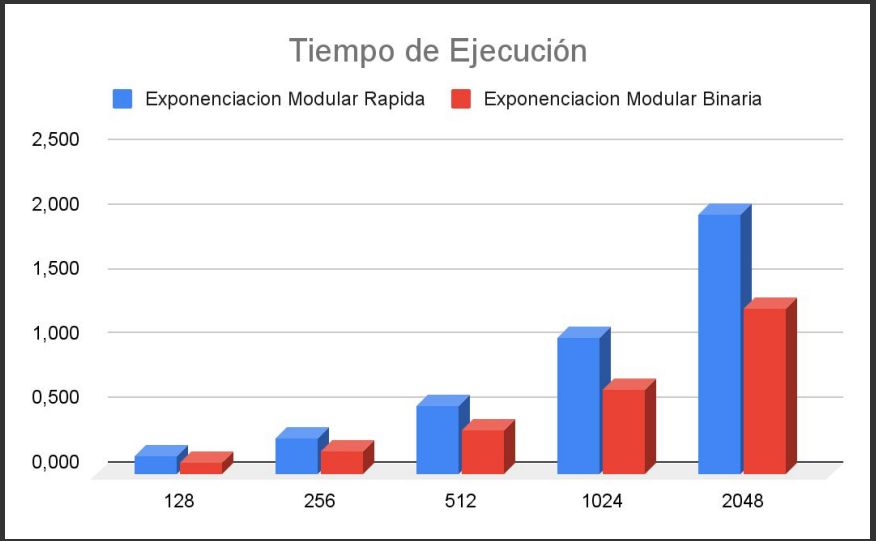
```
ZZ binary_expo_modular(ZZ a, ZZ n, ZZ m){
    ZZ result;
    result = ZZ(1);
    while( n != ZZ(0)) {
        if(!even(n))
            result = MOD(result*a,m);
        a = MOD(a*a,m);
        n >>= 1;
    }
    return result;
}
```

Seguimiento numérico:
572^29 mod 713

r	a	n	m
1	572	29	713
572	630	14	713
572	472	7	713
470	328	3	713
152	634	1	713
113	537	0	713

Comparación:

	Exponenciación Modular Rápida	Exponenciación Modular Binaria	Exponenciación Naive
128	0,135	0,087	∞
256	0,269	0,175	∞
512	0,522	0,339	∞
1024	1,045	0,649	∞
2048	2,004	1,272	∞



Conclusiones:

- El algoritmo de exponenciación binaria es el más eficaz.
- Gran mejora con cierto teoremas implementados.
- Se aprecia cierto grado de similitud entre los algoritmos expuestos.