CIENCIA DE LA COMPUTACIÓN

ÁLGEBRA ABSTRACTA

Tiempo Computacional Algoritmo de Euclides

Choque Mayta, Gabriel Santiago

CCOMP3-1

2021

El alumno declara haber realizado el trabajo de acuerdo a las normas De la universidad Católica San Pablo

Algoritmo de Euclides clásico

Definición

El algoritmo clásico de euclides haya el máximo común divisor de dos números enteros por medio de divisiones euclidianas sucesivas, encadenando el menor de los dos anteriores números junto al residuo positivo de dividir estos dos, hasta que el residuo de los dos números sea 0, entonces el máximo común divisor es el penúltimo resultado de las divisiones euclidianas.

Sustento matemático

La ecuación: A = B*q + R, donde q es coeficiente de A y B.

Si un entero D divide B y R, entonces también divide a A.

Si B = b*D y R = r*D.

La ecuación sería:

A = b*D*q + r*D
A = b*D*q + r*D
A = D(b*q + r), entonces, existe a = A/D.
a*D = D(b*q+r)

Asimismo, si un entero D divide A y B, entonces divide también a R.

De esta observación: mcd(A,B) = mcd(B,R), donde R es el resultado de A mod B

Asumiendo dos números a, b y que a >= b >= 0.
si b = 0, mcd(a,0) = a. sino, b > 0

Tiempo de ejecución vs. Nro. de Bits

128 bits											
	Intentos										Promedio
	1	2	3	4	5	6	7	8	9	10	
Euclides clásico.	0,01	0,009	0,011	0,01	0,009	0,009	0,01	0,009	0,01	0,01	0,0098

512 bits											
	Intentos										Promedio
	1	2	3	4	5	6	7	8	9	10	
Euclides clásico.	0,017	0,013	0,018	0,016	0,021	0,014	0,018	0,015	0,014	0,016	0,0162

1024 bits											
	Intentos										Promedio
	1	2	3	4	5	6	7	8	9	10	
Euclides clásico.	0,017	0,016	0,018	0,017	0,013	0,015	0,016	0,017	0,015	0,013	0,0157

2048 bits											
	Intentos										Promedio
	1	2	3	4	5	6	7	8	9	10	
Euclides clásico.	0,023	0,019	0,02	0,021	0,019	0,024	0,019	0,023	0,021	0,024	0,0213

- Las pruebas las hice con la librería NTL y reemplazando los enteros por números ZZ para probar con números grandes ya que con números pequeños no se ve mucha diferencia.
- El tiempo medido está en segundos.
- Pruebas hechas en CodeBlocks