MILLER-BABIN

Primo = 131 n = 111 561

a = 89

b = 35

a = 85

**Si p es primo y el 0<a<p =>**

15 17

Z15 -> x2=1 {1, 4, 11, 14}

Z17 -> x2=1 {1, 16}

**Si p primo => 1 tiene 2 raíces cuadradas en Zp**

n = 561 a = 89

560 = 2\*2\*2\*2\*35

8935mod561=353 8970mod561=67 89140mod561=1 89280mod561=1 89560mod561=1

as a2s a4s a82 - - a(u-1)\*s

(\*,\*,\*,\*,-1,1,1,- - -,1) Podría ser primo

(\*,\*,\*,\*,\*,1,1,- - -,1) No es primo

(\*,\*,\*,- - -,\*,{1|-1|\*},\_)

El ultimo calculo no es necesario hacerlo. Porque si el penúltimo es asterisco el número no es primo

Cuando calculemos y de n-1 dejamos de calcular por que puede ser que sea primo

Ejemplo

P=111 n-1=110 110=2\*55 u=1

as

a=89 59

SI pasa el test una vez, la probabilidad de fallo es menor 1/4

Función(numero impar)

Calculamos u, s (numero impar)-1=2u\*s

Elegimos a tal que 2<=a<=(numero impar)-2

Calculamos as (mod (numero impar))

Si a ==1 || a==-1

Devuelve p es probable primo

Sino

Para i Desde 1 hasta u-1

a = a2

si a == 1 devuelve p no es primo

si a == -1 devuelve p es probable primo

sino i++

fin para

fin si

devuelve p no es primo

CLAVE PUBLICA

FIRMA DIGITAL