Exemplo:

Considere a operação ***r1 mod r0*** → com r0 > r1. Para ***301 mod 973*** faça:

1. Calcule o **GCD** usando o **Algoritmo de Euclides** (EA).

a) Algoritmo de Euclides considera que:

GCD(r0,r1) = GCD(r0-r1,r1)=GCD(r1,*r0 mod r1*)

Cálculo

gcd(973,301)=gcd(301,70)=gcd(70,21)=gcd(21,7)=gcd(7,0)=7

GCD(973,301) = 7

2. Calcule o **GCD** e $r1^{-1}$ ***mod r0*** (Inverso de r1), se existir, usando o Algoritmo de Euclides Estendido (EEA).

a) Algoritmo de Euclides GCD(r0,r1) = GCD(r1,*r0 mod r1*)=GCD(r1,r2)

r0 = q1*r1 + r2 => r2 = r0 – q1*r1

Generalizando, $r_i = r_{i-2} - q_{i-1} * r_{i-1}$ (I)

b) EEA acrescenta o GCD como uma relação entre r0 e r1, como segue:

GCD(r0,r1) = s*r0 + t*r1

Generalizando, $r_i = s_i * r_0 + t_i * r_1$ (II)

Quando GCD(r0,r1) = 1 existe inverso *mod r0*, então

*(s*r0 + t*r1) = 1 mod r0*

mas *s*r0 mod r0 = 0* então

*t*r1 = 1 mod r0*

Logo, $t = r1^{-1} \bmod r0$ ***(inverso de r1)***

c) **Algoritmo**: a cada passo i do Algoritmo de Euclides calcule ri e escreva como função de r0 e r1:

$r_i = r_{i-2} - q_{i-1} * r_{i-1}$ (I)

$r_i = s_i * r_0 + t_i * r_1$ (II)

Quando $r_i = 0$, r_{i-1} é o GCD e t_{i-1} é o inverso de r_1.

Cálculo para 12 *mod 67* **=> r0 = 67 e r1 = 12**

Passo 0: r0 = 1*r0 + 0*r1 => r0 = 67 , s0 = 1 , t0 = 0

Passo 1: r1 = 0*r0 + 1*r1 => r1 = 12 , s1 = 0 , t1 = 1

Passo 2: gcd(67,12) = gcd(12, **5***12+**7**) => q1 = 5 , r2 = 7

7 = 67 – 5*12 = r0 – q1*r1 => s2 = 1 , t2 = -5 (-q1)

Passo 3: gcd(12,7) = gcd(7,1*7+5) => q2 = 1 , r3 = 5

5 = 12 – 1*7 = r1 – q2*r2

r3 = r1 – 1*(r0-5*r1) = -1*r0 + 6*r1 => s3 = -1 , t3 = 6

Passo 4: gcd(7,5) = gcd(5,1*5+2) => q3 = 1 , r4 = 2

2 = 7 – 1*5 = r2 – q3*r3

r4 = (r0 – 5*r1) – 1*(-1*r0 + 6*r1)

r4 = 2*r0 – 11*r1 => s4 = 2 , t4 = -11

Passo 5: gcd(5,2) = gcd(2,2*2+1) => q4 = 2 , r5 = 1

1 = 5 – 2*2 = r3 – q4*r4

r5 = (-1*r0 + 6*r1) – 2*(2*r0 – 11*r1)

r5 = -5*r0 + 28*r1 => s5 = -5 , t5 = 28

Passo 6: gcd(2,1) = gcd(1,2*1+0) => q5 = 2 , r6 = 0 (FIM)

$r_{i-1} = 1$ => **gcd(67,12) = 1** => são primos relativos, portanto, possui inverso e $\mathbf{t_{i-1} = r_1^{-1} = 28}$

Verificando ...

gcd(67,12) = s5*r0 + t5*r1 = -5*67 + 28*12 = 1

$r1*r1^{-1} = 12*28 = 336 \bmod 67 = 1 \bmod 67$

Generalizando o cálculo de s_i e t_i

$r_i = r_{i-2} - q_{i-1}*r_{i-1}$ e $r_i = s_i*r_0 + t_i*r_1$

$r_i = (s_{i-2}*r_0 + t_{i-2}*r_1) - q_{i-1}*(s_{i-1}*r_0 + t_{i-1}*r_1) = (s_{i-2} - q_{i-1}*s_{i-1})*r_0 + (t_{i-2} - q_{i-1}*t_{i-1})\, r_1$

$\boldsymbol{s_i = s_{i-2} - q_{i-1}*s_{i-1}}$ (III)

$\boldsymbol{t_i = t_{i-2} - q_{i-1}*t_{i-1}}$ (IV)