$$\begin{array}{l} MCD(a,b) \\ a \geq b \geq 0 \\ b \neq 0 \end{array} = \begin{cases} MCD(b, a \bmod b) & b > 0 \\ a & b = 0 \end{cases}$$

Prop: $a \geq b \geq 0$ y $b \neq 0$

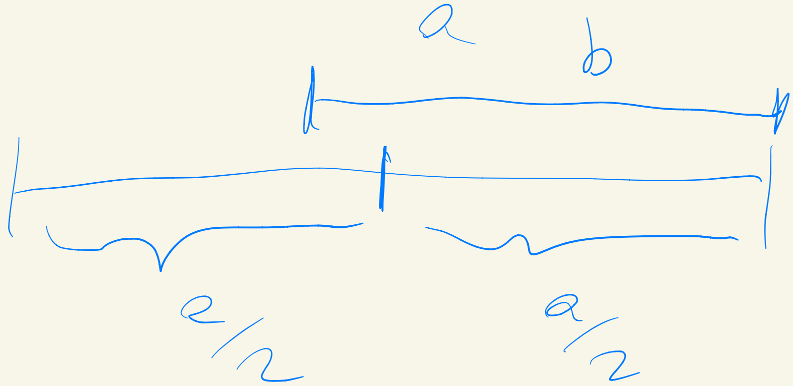
$$MCD(b, a \bmod b) < \frac{a}{2}$$

Dem: $b = \frac{a}{2} \Rightarrow a \bmod b = 0 < \frac{a}{2}$

$b < \frac{a}{2} \Rightarrow a \bmod b < b < \frac{a}{2}$ //

$$\boxed{b > \frac{a}{2}} \Rightarrow -b < -\frac{a}{2}$$

$$a \bmod b = a - b$$




$$a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2} \,//$$

— . —

Algoritmo extendido de Euclides $\quad s, t \in \mathbb{Z}$

$$\underline{MCD(a, b) = s \cdot a + t \cdot b}$$

$a = r_0$

$b = r_1$

$a \bmod b = r_2$

$\vdots$

$r_{i-1}$

$r_i$

$r_{i+1} = r_{i-1} \bmod r_i$

$\vdots$

$r_{k-1} = MCD(a, b)$

$\boxed{r_k = 0}$

$$a = r_0 = 1 \cdot a + 0 \cdot b$$

$$b = r_1 = 0 \cdot a + 1 \cdot b$$

$$r_2$$

$$\vdots$$

$$r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$$

$$r_i = s_i \cdot a + t_i \cdot b$$

$$r_{i+1} = s_{i+1} \cdot a + t_{i+1} \cdot b$$

$$r_{i+1} = r_{i-1} \bmod r_i$$

$$r_{i-1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + \underbrace{r_{i-1} \bmod r_i}_{r_{i+1}}$$

$$\boxed{r_{i+1} = r_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i}$$

$$r_{i+1} = r_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i$$

$$= (s_{i-1} \cdot a + t_{i-1} \cdot b)$$

$$- \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot (s_i \cdot a + t_i \cdot b)$$

$$= \left(s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i\right) \cdot a$$

$$+ \left(t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor t_i\right) \cdot b$$

$$\boxed{\begin{aligned} s_{i+1} &= s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i \\ t_{i+1} &= t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i \end{aligned}}$$

$$103 = 1 \cdot 103 + \boxed{0} \cdot 86$$

$$86 = \boxed{0} \cdot 103 + 1 \cdot 86$$

$$17 = \boxed{1} \cdot 103 + (-1) \cdot 86$$

$$\boxed{1 = (-5)\, 103 + 6 \cdot 86}$$

$$0 - \left\lfloor \frac{86}{17} \right\rfloor \cdot 1 \qquad 1 - \left\lfloor \frac{86}{17} \right\rfloor \cdot (-1)$$

$$\boxed{0} \qquad 0 - \left\lfloor \frac{103}{86} \right\rfloor \cdot 1 = -1$$

Cor: $\forall a \geq b \geq 0$, $a \neq 0$ existe $s, t \in \mathbb{Z}$:

$$MCD(a,b) = s \cdot a + t \cdot b$$

Inverso modular

$b$ es inverso de $a$ en modulo $n$ si

$$a \cdot b \equiv 1 \mod n$$

Ejemplo

$$5 \cdot 5 \equiv 1 \mod 8$$

$$5 \cdot 2 \equiv 1 \mod 9$$

$$\cancel{2 \cdot x \equiv 1 \mod 8}$$

$\underline{5} \cdot \underline{5} \equiv 1 \mod 8$

$5 \cdot \underline{13} \equiv 1 \mod 8$

$5 \equiv 13 \mod 8$

$\{0, \ldots, 7\}$

Teo: $a$ tiene inverso en módulo $n$ ssi $\boxed{MCD(a,n) = 1}$

$\Leftarrow$

$\Rightarrow$?

$\boxed{MCD(a,n) = 1}$

$$MCD(a,n) = s \cdot a + t \cdot n$$

$$\therefore \boxed{1 = s \cdot a + t \cdot n}$$

$$\boxed{1 \equiv s \cdot a \mod n}$$

$103, 86$

Inverso de 86 en módulo 103:

$$\mathrm{MCD}(103, 86) = 1 = -5 \cdot 103 + \boxed{6 \cdot 86}$$

$$6 \cdot 86 \equiv 1 \mod 103$$

$$(-5)\,103 \equiv 1 \mod 86$$

$$(81) \cdot 103 \equiv 1 \mod 86$$

$$81 \equiv -5 \mod 86$$

$$(86 \mid 81 - (-5))$$

# RSA

$A \to p_A, s_A$

$c := Enc(p_A, m)$

$m := Dec(s_A, c)$

- Generar al azar dos números primos $P, Q$ $\quad 10^{199} \leq P \leq 10^{200} - 1$
- $N = P \cdot Q$
- $\phi(N) = (P-1) \cdot (Q-1)$
- generar al azar un número $d$ tal que $\boxed{MCD(d, \phi(N)) = 1}$
- Construir $e$ tal que $e$ es inversa del $d$ en módulo $\phi(N)$

$$\boxed{e \cdot d \equiv 1 \mod \phi(N)}$$

$p_A = (e, N) \qquad s_A = (d, N)$

$$\mathrm{Enc}((e,N),m) = m^e \bmod N$$

$$m \in \{0, \dots, N-1\}$$

$$\mathrm{Dec}((d,N),c) = c^d \bmod N$$

$$P = 13 \quad , \quad Q = 19$$

$$N = 13 \cdot 19 = 247$$

$$\phi(N) = (13-1)\cdot(19-1) = \underline{216}$$

$$d = 65 \qquad e = 113$$

$$P_A = (\underbrace{113}_{e}, \underbrace{247}_{N}) \qquad S_A = (\underbrace{65}_{d}, \underbrace{247}_{N})$$

$$m \longmapsto m^{113} \bmod 247$$

$$c \longmapsto c^{65} \bmod 247$$

$\pi(n)$: número de primos menores o iguales a $n$

$$\pi(10) = 4$$

$$\boxed{\lim_{n\to\infty} \frac{\pi(n)}{\left(\frac{n}{\ln n}\right)} = 1}$$

$$x \in \{1, \ldots, n\}$$

$$\Pr(x \text{ primo}) = \frac{\pi(n)}{n} \approx \frac{\frac{n}{\ln n}}{n} = \frac{1}{\ln n}$$

$$\Pr(X \text{ sea primo}) \approx \frac{1}{\ln 10^{200}}$$

$$X \in \{1, \ldots, 10^{200}\} = \frac{1}{460}$$

$$X = i$$

$$\Pr(X = i) = \left(1 - \frac{1}{460}\right)^{i-1} \cdot \frac{1}{460}$$

$$X \sim \mathrm{GEO}\left(\frac{1}{460}\right) \qquad X \sim \mathrm{GEO}(p)$$

$$E[X] = \frac{1}{p} = 460$$

$$\Pr(X \text{ sea primo}) = \frac{\pi(n-1) - \pi(m-1)}{n-m}$$

$$X \in \{m, \ldots, n-1\}$$

$$10^{199} \leq X < 10^{200}$$

$$n = 10^{200}$$

$$m = 10^{199}$$

$$\approx \boxed{\frac{\dfrac{n-1}{\ln n-1} - \dfrac{m-1}{\ln m-1}}{n-m}}$$