EXERCISE 2 Show that the multiplicative inverse a^{-1}, $a \in \mathbb{Z}_n^*$ is unique.

(Hint: first prove that

$$a, b, n \in \mathbb{Z}^+ : (n \mid ab) \wedge (\gcd(a,n)=1) \Rightarrow (n \mid b)$$

)

1) $n \mid ab \Rightarrow \exists k \in \mathbb{Z}^+ : ab = kn$
2) $\gcd(a,n)=1 \Rightarrow \exists x, y \in \mathbb{Z} : 1 = ax + ny$

$$\Downarrow$$

$$b = bax + bny = knx + bny = (kx + by)n \Rightarrow \exists k' \in \mathbb{Z}^+ : b = k'n \Rightarrow n \mid b$$

a^{-1} unico $\Rightarrow \exists x_1, x_2 : ax_1 \equiv 1 \bmod n,\ ax_2 \equiv 1 \bmod n \Rightarrow [x_1]_n = [x_2]_n$

$ax_1 \equiv ax_2 \bmod n \Leftrightarrow a(x_1 - x_2) \equiv 0 \bmod n \Rightarrow \exists k : a(x_1 - x_2) = kn \Rightarrow$

$\Rightarrow n \mid a(x_1 - x_2) \wedge a \in \mathbb{Z}_n^* (\Rightarrow \gcd(a,n)=1) \Rightarrow n \mid (x_1 - x_2) \Rightarrow$

$\Rightarrow \exists h \in \mathbb{Z} : x_1 - x_2 = hn \Rightarrow x_1 = x_2 + hn \Rightarrow [x_1]_n = [x_2]_n = [a]_n^{-1}$ ∎

EXERCISE 3

For $a, b > 0$ define their least common multiple $\text{lcm}(a,b) = \min\{c > 0 : (a \mid c) \wedge (b \mid c)\}$

Show that $\text{lcm}(a,b) \cdot \gcd(a,b) = a \cdot b$

and discuss the algorithmic implications

$d \mid a \Rightarrow d \mid ab \Rightarrow \exists k : ab = kd \Rightarrow$ dimostriamo $k \leq m$:

1) $d \mid a \Rightarrow a = h_1 d$, $d \mid b \Rightarrow b = h_2 d \Rightarrow ab = h_1 d b = a h_2 d = dk \Rightarrow$
$\Rightarrow k = h_1 b = a h_2 \Rightarrow b \mid k$, $a \mid k \Rightarrow k \geq m$ ■

2) $m = \text{lcm}(a,b) \Rightarrow \exists r, s \in \mathbb{Z}^+ : m = ar, bs$
$d = \gcd(a,b) = ax + by \quad (x, y \in \mathbb{Z})$
$md = m(ax + by) = max + mby = abs x + abr y = (sx + ry)ab$
$t = sx + ry \Rightarrow md = abt = kdt \Rightarrow m = kt \Rightarrow k \mid m \Rightarrow k \leq m$ ■

```
lcm(a,b):
    d ← EUCLID(a,b)
    (m,r) ← R_QR(ab,d)   // r = 0
    return m
```

$T_{\text{lcm}}(|\langle a,b \rangle|) = T_{\text{EUCLID}}(|\langle a,b \rangle|) + O(|\langle a,b \rangle|^2) + T_{\text{R\_QR}}(|\langle ab,d \rangle|) = O(|\langle a,b \rangle|^3)$

EXERCISE 4 Let $n \geq 3$. Determine the exact number of recursive calls (including the external one) executed by

$$EUCLID(F_n, F_{n-1})$$

where F_i, $i \geq 1$, is the i-th Fibonacci number and evaluate the running time of the call as a function of $|\langle F_n, F_{n-1} \rangle|$

$EU(F_3, F_2) = EU(2,1) \to EU(1,0) \to 1 \Rightarrow n=3$: 2 chiamate
$EU(F_4, F_3) = EU(3,2) \to EU(2,1) \Rightarrow n=4$: 3 //

$EU(F_n, F_{n-1})$: $n-1$ chiamate per $n \geq 3$ (non-vale per $EU(F_2, F_1)$)
Caso induttivo:
$EU(F_n, F_{n-1}) \to EU(F_{n-1}, F_n \bmod F_{n-1}) \Rightarrow$ dimostriamo $F_n \bmod F_{n-1} = F_{n-2}$:
division theorem: $\exists! q, r: F_n = qF_{n-1} + r$, $r \in [0, F_{n-1})$
$q=1$, $r = F_{n-2} < F_{n-1} \Rightarrow F_n = F_{n-1} + F_{n-2}$ ✓
$EU(F_n, F_{n-2}) \to EU(F_{n-1}, F_{n-2}) \Rightarrow n-1$ chiamate ■

T_{EU}:
$n-1$ chiamate $\Rightarrow$ calcolo $F_{i-2} = F_i \bmod F_{i-1}$
$F_i = \Theta\left(\left(\frac{1+\sqrt{5}}{2}\right)^i\right) \to \log_2 F_i = \Theta(\log c^i) = \Theta(i)$

$T_{A\_OR} = (|\langle a,b \rangle|) = O(|\langle a,b \rangle|^2)$
↑
$O(i^2) \Rightarrow$ running time: $\sum_{i=1}^{n-1} O(i^2) = O(n^3)$

EXERCISE 5 Prove that:

For given $a, b, c \in \mathbb{Z}$, the equation (in $x, y \in \mathbb{Z}$):

$$ax + by = c$$

has solutions if and only if

$$\gcd(a, b) \mid c$$

1) $\Leftarrow$: $d = \gcd(a,b) = \min\{z > 0 : z = ax + by,\ x, y \in \mathbb{Z}\} = a\bar{x} + b\bar{y}$

$c = kd = k(a\bar{x} + b\bar{y}) = a(k\bar{x}) + b(k\bar{y}) = ax' = by'$ (una delle soluzioni)

2) $\Rightarrow$: $\exists x', y' : c = ax' + by'$

contr.: $\gcd(a,b) = d \mid c \Rightarrow c = qd + r,\ r \in [0, d] \Rightarrow r > 0$

Bezout su $d = \gcd(a,b)$

$qd + r = ax' + by' \Rightarrow r = ax' + by' - q(a\bar{x} + b\bar{y}) = a(x' - q\bar{x}) + b(y' - q\bar{y}) \Rightarrow$

$\Rightarrow$ contraddizione ■

EXERCISE 6 Find all possible pairs $(x,y) \in \mathbb{Z} \times \mathbb{Z}$:

$$d = \gcd(a,b) = ax + by$$

① $d = a\bar{x} + b\bar{y}$ ("base")

② $d = ax' + by'$

$\Rightarrow a(x'-\bar{x}) + b(y'-\bar{y}) = 0 \Rightarrow (d \mid a) \wedge (d \mid b) \Rightarrow$

$\Rightarrow \frac{a}{d}(x'-\bar{x}) + \frac{b}{d}(y'-\bar{y}) = 0 \Rightarrow \frac{a}{d}(x'-\bar{x}) = \frac{b}{d}(\bar{y}-y') \Rightarrow$

$d = a\bar{x} + b\bar{y} \Rightarrow 1 = \frac{a}{d}\bar{x} + \frac{b}{d}\bar{y} \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

$\frac{a}{d}(x'-\bar{x}) = \frac{b}{d}(\bar{y}-y') = k\frac{b}{d} \Rightarrow \frac{b}{d} \mid \frac{a}{d}(x'-\bar{x}) \Rightarrow \frac{a}{d}(x'-\bar{x}) \bmod \frac{b}{d} = 0 \wedge$

$\wedge \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \Rightarrow x'-\bar{x} = h_1\frac{b}{d} \Rightarrow x' = \bar{x} + h_1\frac{b}{d}$

Simmetrico: $y' = \bar{y} - h_2\frac{a}{d}$

$d = a\bar{x} + b\bar{y} = a\left(x' - h_1\frac{b}{d}\right) + b\left(y' + h_2\frac{a}{d}\right) = ax' - h_1\frac{ab}{d} + by' + h_2\frac{ab}{d} \Rightarrow$

$\Rightarrow 0 = (h_2 - h_1)\frac{ab}{d} \Rightarrow h_1 = h_2$

$x' = \bar{x} + h\frac{b}{d}, \quad y' = \bar{y} - h\frac{a}{d}$