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

(Hint: first prove that

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

EXERCISE 3

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

Show that

$$\operatorname{lcm}(a,b) \cdot \gcd(a,b) = a \cdot b$$

and discuss the algorithmic implications

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 $|\langle F_n, F_{n-1} \rangle|$

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

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

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

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