Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Primer semestre 2025**
Instituto de Matemática y Estadística

PRÁCTICO 2: MÁXIMO COMÚN DIVISOR, ALGORITMO DE EUCLIDES E IDENTIDAD DE BÉZOUT.

Ejercicio 1.

a. Hallar los divisores positivos de 21 y de 30.

b. Hallar los divisores positivos comunes de 21 y 30.

c. Usando lo anterior, calcular el máximo común divisor de 21 y 30.

Ejercicio 2. [Algoritmo de Euclides]. Sean $a, b \in \mathbb{Z}$.

a. Probar que si $d|a$ y $d|b$, entonces $d|(ax + by)$, para todo $x, y \in \mathbb{Z}$.

b. Probar que $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, a - bq)$, para todo $q \in \mathbb{Z}$.

c. Describir el Algoritmo de Euclides para calcular el $\operatorname{mcd}(a, b)$.

d. Usar el Algoritmo de Euclides para calcular el $\operatorname{mcd}(a, b)$ en los siguientes casos:

i) $a = 63$, $b = 15$.
ii) $a = 455$, $b = 1235$.
iii) $a = 2366$, $b = 273$.

Ejercicio 3. [Lema de Euclides]. Sean $a, b, c \in \mathbb{N}$, tales que $\operatorname{mcd}(a, b) = 1$ (a y b son primos entre sí). Probar o dar un contraejemplo de las siguientes afirmaciones.

a. Si $a|(bc)$ entonces $a|c$.

b. Si $a|c$ y $b|c$ entonces $ab|c$.

c. ¿Valen las partes anteriores si $\operatorname{mcd}(a, b) \neq 1$?

Ejercicio 4. [Bézout] Sean $a, b, c \in \mathbb{N}$. Probar las siguientes afirmaciones:

a. $\operatorname{mcd}(ca, cb) = c \operatorname{mcd}(a, b)$. Sugerencia: usar Bézout y probar la doble desigualdad.

b. Si $c|a$ y $c|b$ entonces: $\operatorname{mcd}(a/c, b/c) = \operatorname{mcd}(a, b)/c$.

c. Si a y b son primos entre sí, entonces: $\operatorname{mcd}(a - b, a + b) = 1$ o 2. Sugerencia: probar primero que $\operatorname{mcd}(a - b, a + b)$ divide a $\operatorname{mcd}(2a, 2b)$.

Ejercicio 5. Para este ejercicio será útil la siguiente propiedad: si $d|a$ y $d|b$, entonces $d|(ax+by)$, $\forall\, x, y \in \mathbb{Z}$.

a. Se define la sucesión de Fibonacci como $F_0 = 0$, $F_1 = 1$ y $F_{n+2} = F_{n+1} + F_n$ para todo $n \geq 0$. Demostrar que dos términos consecutivos cualesquiera de la sucesión de Fibonacci son coprimos.

b. Demostrar que $\operatorname{mcd}(7k + 3, 12k + 5) = 1$, para todo $k \in \mathbb{N}$.

c. Sean $a, b, c, d \in \mathbb{N}$, tales que $(ad-bc)|a$ y $(ad-bc)|c$. Probar que: $\operatorname{mcd}(an+b, cn+d) = 1$, $\forall\, n \in \mathbb{N}$. Sugerencia: hallar una combinación entera de $an + b$ y $cn + d$ que valga $ad - bc$. Luego adaptarla para que valga 1.

Ejercicio 6. [Cofactores.] Sean $a, b \in \mathbb{Z}$ no nulos.

a. Probar que $d = \text{mcd}(a, b)$, si y sólo si, existen $a^*, b^* \in \mathbb{Z}$, coprimos, tales que: $a = da^*$ y $b = db^*$. Los enteros a^* y b^* se denominan cofactores de a y b. Sugerencia: usar Bézout.

b. Hallar los cofactores de $a = 63$ y $b = 15$.

c. Probar que si a es par y b impar entonces: $\text{mcd}(a, b) = \text{mcd}(a/2, b)$. Sugerencia: usar cofactores.

Ejercicio 7. En cada caso, hallar $a, b \in \mathbb{N}$ que verifiquen las condiciones dadas.

a. $ab = 22275$ y $\text{mcd}(a, b) = 15$. Sugerencia: usar cofactores y factorizar en producto de primos.

b. $ab = 1008$ y $\text{mcm}(a, b) = 168$. Recordar que: $\text{mcm}(a, b) \cdot \text{mcd}(a, b) = |a||b|$, $\forall\ a, b \in \mathbb{Z}$.

c. $a + b = 1271$ y $\text{mcm}(a, b) = 330 \cdot \text{mcd}(a, b)$.

d. $a + b = 122$ y $\text{mcd}(a, b) + \text{mcm}(a, b) = 1802$.

Ejercicio 8. Hallar $\text{mcd}(a, b)$ sabiendo que $\text{mcd}(a, b) \cdot \text{mcm}(a, b) = 48$ y $a^2 = b^2 + 28$.