1. Algoritmo Euclides

Lema 1.1. $\forall a, b, q, r \in \mathbb{Z} \land a = bq + r \Longrightarrow \operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$

Prueba: Tenemos que

$$
\begin{aligned}
a &= bq + r \\
r &= a - bq
\end{aligned}
$$

Probemos que a y b tienen los mismos divisores comunes que b y r. Así $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$

- Supongamos que $d|a \land d|b; \quad d \in \mathbb{Z}$
  Luego por teorema $d|bq$
  Luego por teorema $d|(a - bq)$
  Ahora $r = a - bq$
  $\therefore d|r$
- Supongamos que $d|b \land d|r$
  Luego $d|(bq + r)$
  Ahora $a = bq + r$
  $\therefore d|a$

Por lo tanto hemos probado que cualquier divisor común de b y r también es divisor común de a y b
$\therefore \operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$ □

1.1. Ejemplos Algoritmo de Euclides

Pregunta: Hallar el $\operatorname{mcd}(287, 91)$

Respuesta: Dividir el mas grande entre el mas pequeño $287 \div 91$, por algoritmo de la division $287 = 91 \cdot 3 + 14$.

Fijémonos que cualquier divisor de 91 y 287 debe ser un divisor de $14 = 287 - 91 \cdot 3$ de modo que si d es un divisor de 91 y 287 entonces

$$287 = d \cdot q_1 \land 91 = d \cdot q_2$$

Luego

$$
\begin{aligned}
14 &= 287 - 91 \cdot 3 \\
&= d \cdot q_1 - d \cdot q_2 \cdot 3 \\
&= d(q_1 - q_2 \cdot 3)
\end{aligned}
$$

Es decir, d es un divisor de 14

De igual forma se prueba que cualquier divisor de 91 y 14 debe ser un divisor de 287

Por lo tanto $\operatorname{mcd}(287, 91) = \operatorname{mcd}(91, 14)$

Hallar $\operatorname{mcd}(91, 14)$

$$
\begin{aligned}
91 &= 14 \cdot 6 + 7 \\
91 - 14 \cdot 6 &= 7
\end{aligned}
$$

Cualquier divisor de 91 y 14 también divide a 7 y cualquier divisor común de 14 y 7 divide a 91, luego

$$\operatorname{mcd}(91, 14) = \operatorname{mcd}(14, 7)$$

Y continua de la misma forma:

$$14 = 7 \cdot 2$$

Luego $\operatorname{mcd}(14, 7) = 7$

Por lo tanto

$$\operatorname{mcd}(287, 91) = \operatorname{mcd}(91, 14) = \operatorname{mcd}(14, 7) = 7$$

En conclusion, el algoritmo de Euclides para hallar el mcd de dos enteros a y b utiliza divisiones sucesivas hasta que uno de los enteros se haga cero (residuo 0)