

The Euclidean Algorithm

Let E be a Euclidean domain with $v: E \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$

Let $a, b \in E$, $b \neq 0$. Initialize $r_0 = a$ and $r_1 = b$.

$$r_0 \div r_1 : \quad r_0 = q_2 r_1 + r_2 \quad r_2 \neq 0 \quad v(r_2) < v(r_1)$$

$$r_1 \div r_2 : \quad r_1 = q_3 r_2 + r_3 \quad r_3 \neq 0 \quad v(r_3) < v(r_2)$$

\vdots

$$r_{n-2} \div r_{n-1} : \quad r_{n-2} = q_n r_{n-1} + r_n \quad r_n \neq 0 \quad v(r_n) < v(r_{n-1})$$

$$r_{n-1} \div r_n : \quad r_{n-1} = q_{n+1} r_n + r_{n+1} \quad r_{n+1} = 0$$

Claim r_n is a $\gcd(a, b)$.

Proof (i) Show $r_n | r_1 = b$ and $r_n | r_0 = a$

(ii) Show $d | r_0$ and $d | r_1 \Rightarrow d | r_n$

Claim n is finite (the algorithm terminates).

Proof $v(b) = v(r_1) > v(r_2) > v(r_3) > \dots \geq 0$

Therefore a $\gcd(a, b \neq 0)$ exists in E .