PGCD de $X^n - 1$ et $X^m - 1$ où $m \in \mathbb{N}$, $n \in \mathbb{N}$ avec $0 < m < n$.

- $P_k(X) := X^k - 1$ pour $k \in \mathbb{N}^*$.
- $Q_{m,n}(X) := P_m(X) \wedge P_n(X)$ (pgcd).
- $P_n(X) = X^m (X^{n-m} - 1) + X^m - 1$
  $= X^m P_{n-m}(X) + P_m(X)$

  Donc $Q_{m,n}(X)$ divise $X^m P_{n-m}(X)$.
- $Q_{m,n}(X) \wedge X^m = 1$ car sinon $X \mid Q_{m,n}(X) \mid X^n - 1$, ce qui est faux.
- Donc $Q_{m,n}(X)$ divise $P_{n-m}(X)$, et donc (aussi) $P_n(X) \wedge P_{n-m}(X)$, ie $Q_{m,n}(X)$ divise $Q_{m-n,n}(X)$.
- $Q_{m-n,n}(X)$ divise $Q_{m,n}(X)$ via $P_m(X) = P_n(X) - X^m P_{n-m}(X)$.
- Donc $Q_{m,n}(X) = Q_{m-n,n}(X)$ d'où $Q_{m,n}(X)$ est égal à $P_{m \wedge n}(X)$ via l'algo. des différences.

⚠ Noter que $Q_{k,k}(X) = P_k(X)$, ou $Q_{k,0}(X) = P_k(X)$.

ⓘ Le raisonnement s'adapte à $2^n - 1$ et $2^m - 1$ très facilement, et même à $p^n - 1$ et $p^m - 1$ si $p \in \mathbb{P}$.