Criteri di divisibilità

RSA

- $p, q \in \mathbb{P} \mid p \neq q \quad n := pq,\ \lambda(n) := \text{mcm}(p-1, q-1)$
  - $\lambda(n) \Big| \varphi(n) = (p-1)(q-1)$ poiché $p, q \in \mathbb{P}$ **!!! NON CAPISCO**
- $\text{MCD}(a, n) = 1 \iff p \nmid a \wedge q \nmid a \implies a^\lambda(n) \equiv 1 \pmod{n}$
  - $\lambda(n)$ per definizione $\implies \exists i, j \in \mathbb{Z} \mid \lambda(n) = (p-1) \cdot i = (q-1) \cdot j$
  - $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$ per il piccolo teorema di Fermat
  - **!!! NON HO CAPITO NIENTE**
- **procedimento per RSA**
  - $p \neq q \in \mathbb{P}$ **molto grandi**
  - $n := pq$
  - $\lambda(n) := \text{mcm}(p-1, q-1)$
  - $e \mid 1 < e < \lambda(n) : \text{MCD}(e, \lambda(n)) = 1 \implies [e] \in \mathbb{Z}^*_{\lambda(n)}$
    - si trova un'identità di Bézout per e e $\lambda(n)$ del tipo $1 = e \cdot d + \lambda(n) \cdot k$ per certi d, k, ma per definizione quest'identità implica che $ed \equiv 1 \pmod{\lambda(n)}$
  - $d := e^{-1} \pmod{\lambda(n)}$ viene calcolato tramite l'algoritmo di Euclide
  - n, e **pubbliche**, d **privata**
    - n, d, e sono tali che $(a^e)^d \equiv a \pmod{n},\ \text{MCD}(a, n) = 1$
      - $\begin{cases} ed \equiv 1 \pmod{\lambda(n)} \\ a^{\lambda(n)} \equiv 1 \pmod{n} \end{cases}$
      - **!!! NON HO CAPITO NIENTE**