Vérification · CE.

1. $w = s^{-1} \pmod q$.
2. $u_1 = w \cdot h(x) \pmod q$
3. $u_2 = w \cdot r \pmod q$.
4. $P = u_1 A + u_2 B$.
5. $\text{Ver}_{\text{pub}}(x, (r,s))$!

$x_P \begin{cases} \equiv r \pmod q & \text{valide} \\ \not\equiv r \pmod q & \text{invalide} \end{cases}$

- **Exercice** Montrer que l'algo. de vérification est correcte.
  (i.e. que (r,s) vérifie $x_P \equiv r \pmod q$).

→ • Trouver une Courbe elliptique n'est pas facile.
  (NIST a standardisé 6 pt).
  • Les Calculs sont standards.
  • La sécurité repose sur le PLD des Courbes elliptiques.
  La meilleur attaque est en $O(\sqrt{q})$.