Structure de groupe

$(\mathscr{C}, +)$ a les propriétés suivantes

- Fermeture $\forall P, Q \in \mathscr{C}$

  $$P + Q \in \mathscr{C}$$

- Associativité $\forall P, Q, R \in \mathscr{C}$

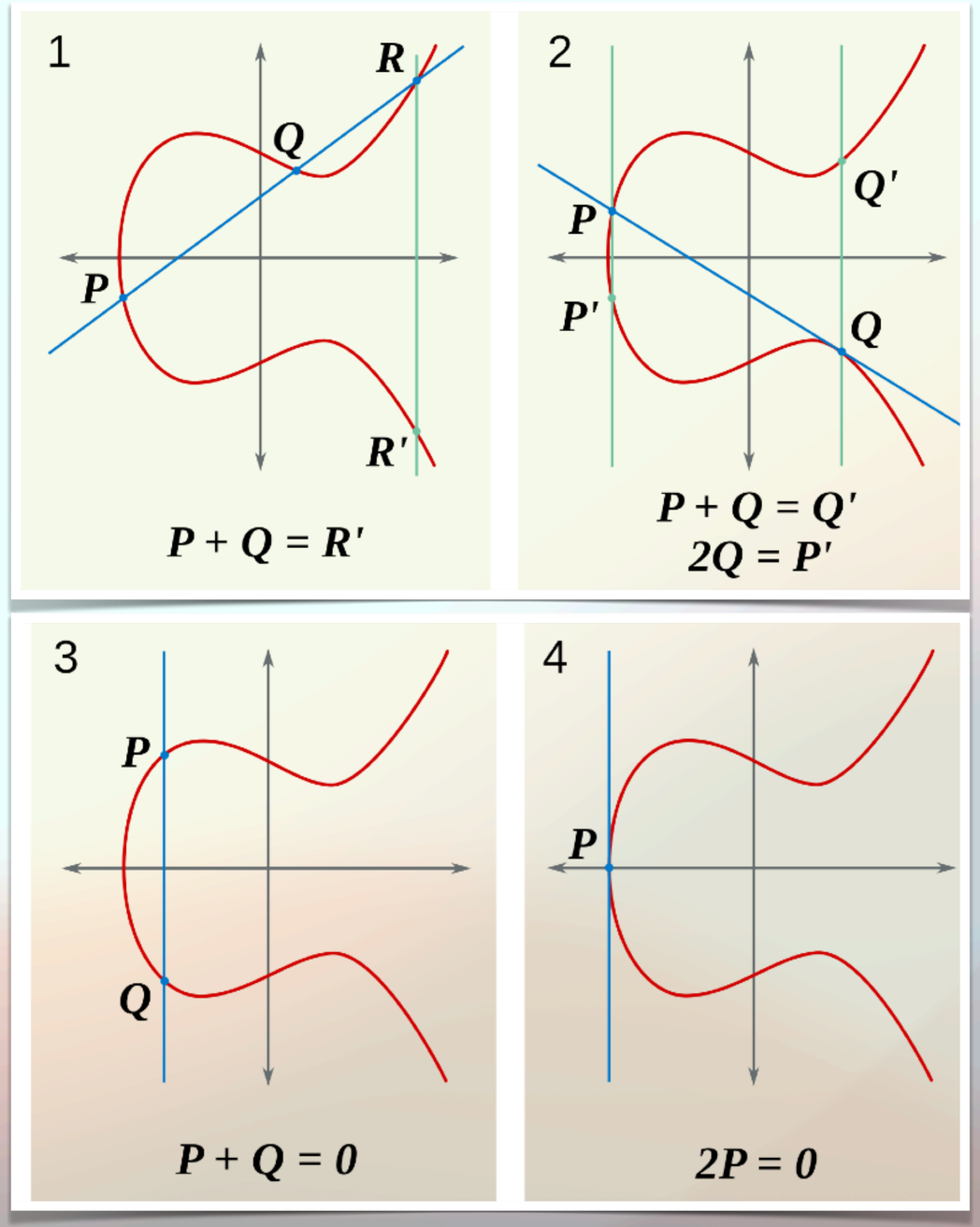
  $$(P + Q) + R = P + (Q + R)$$

- Identité $\forall P \in \mathscr{C}$

  $$\mathcal{O} + P = P = P + \mathcal{O}$$

- Inverse $\forall P \in \mathscr{C}, \exists Q \in \mathscr{C}$

  $$P + Q = \mathcal{O}$$



Addition et doublement

(Aka *square and multiply*)

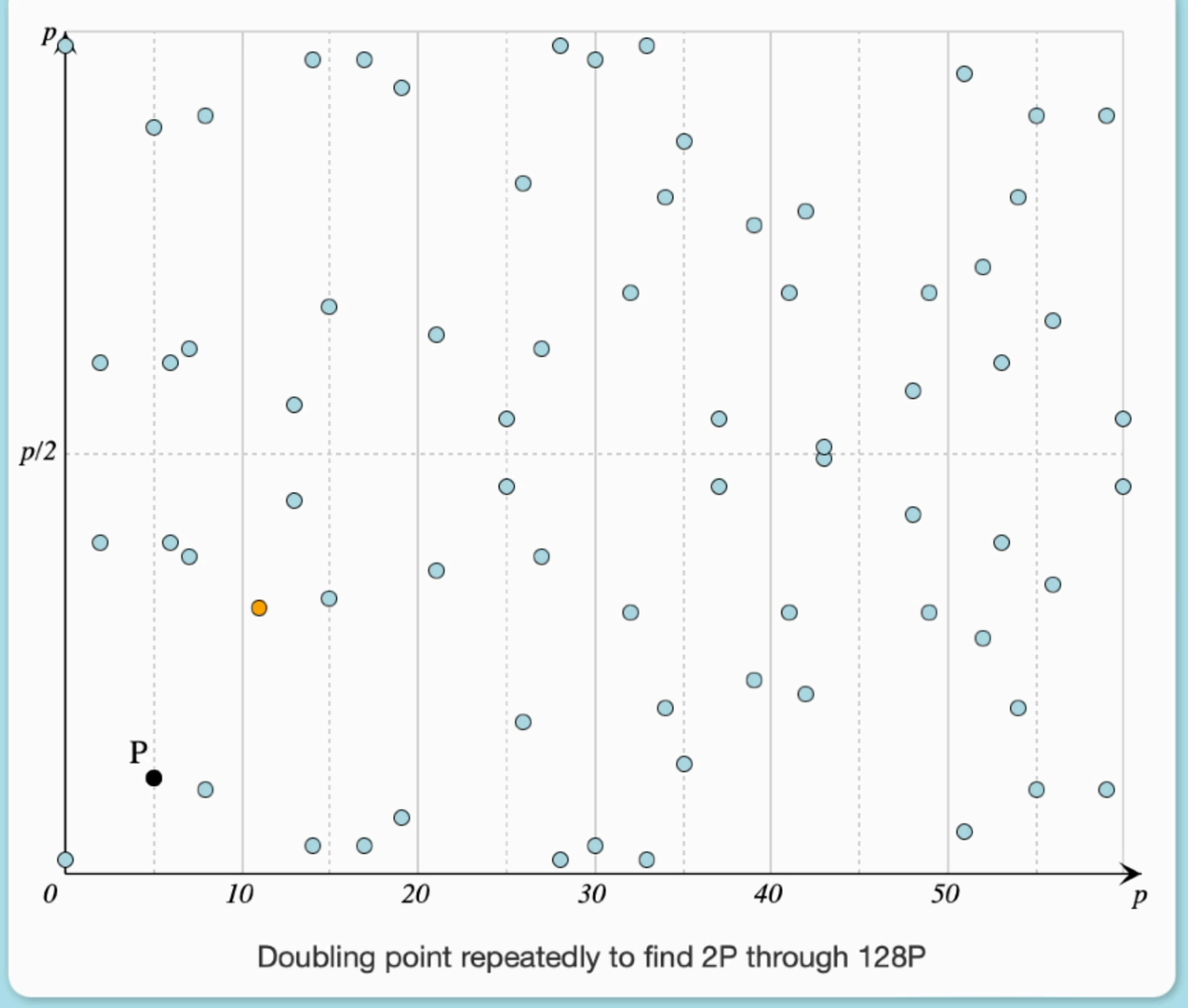
- Doubler P à répétition

$$\{P, 2P, 4P, 8P, 16P, \ldots\}$$

- Additionner les points nécessaires pour obtenir le multiple de P désiré

Exemple: 100P = 64P + 32P + 4P

Plutôt que d'additionner 100 fois ($O(n)$), il suffit de doubler 6 fois et additionner 3 fois (donc un total de 9 additions, $O(log(n))$)



Double-and-add method for point 153P