(Aka *square and multiply*)

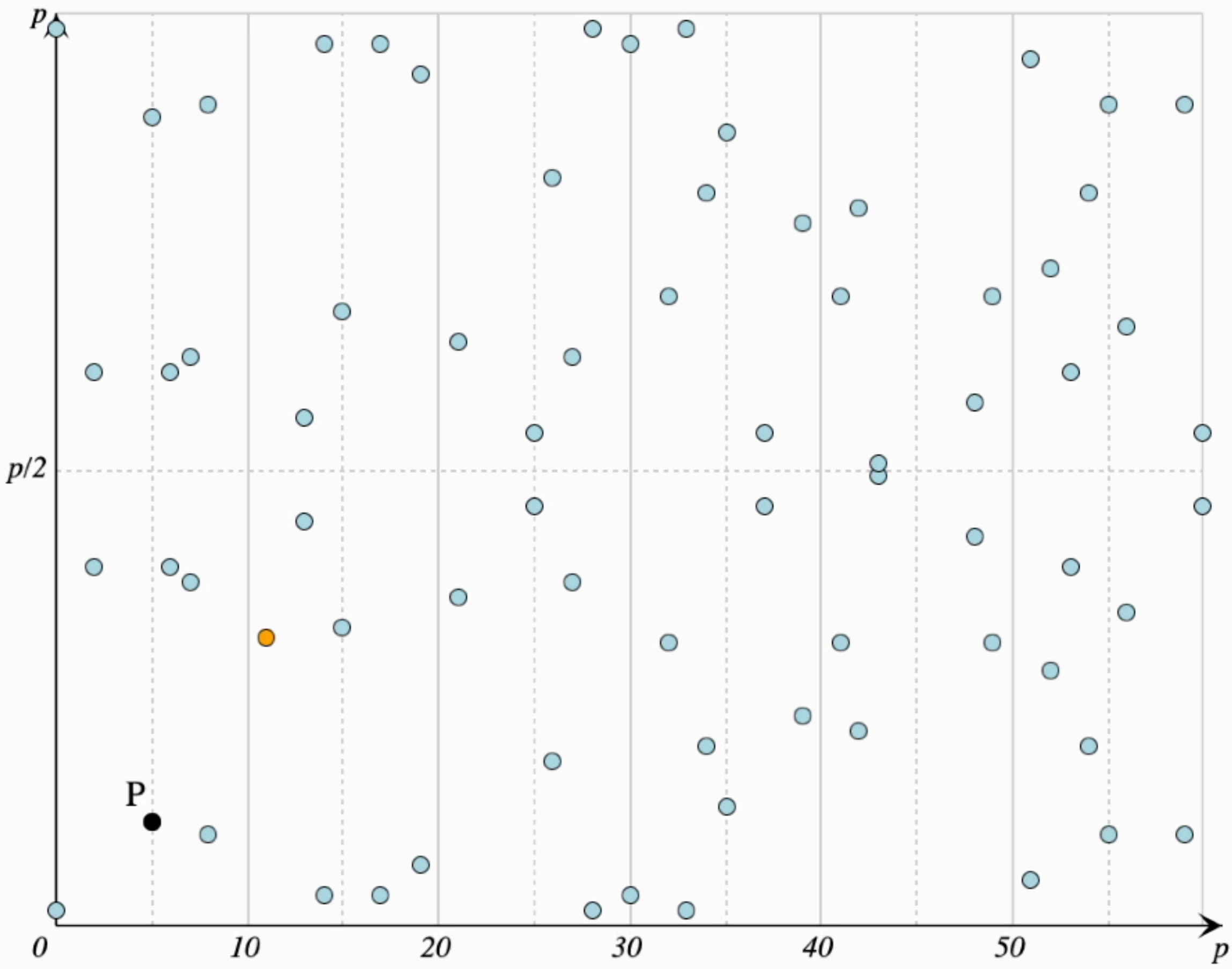
- Doubler P à répétition

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

- 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, $O(log(n))$)

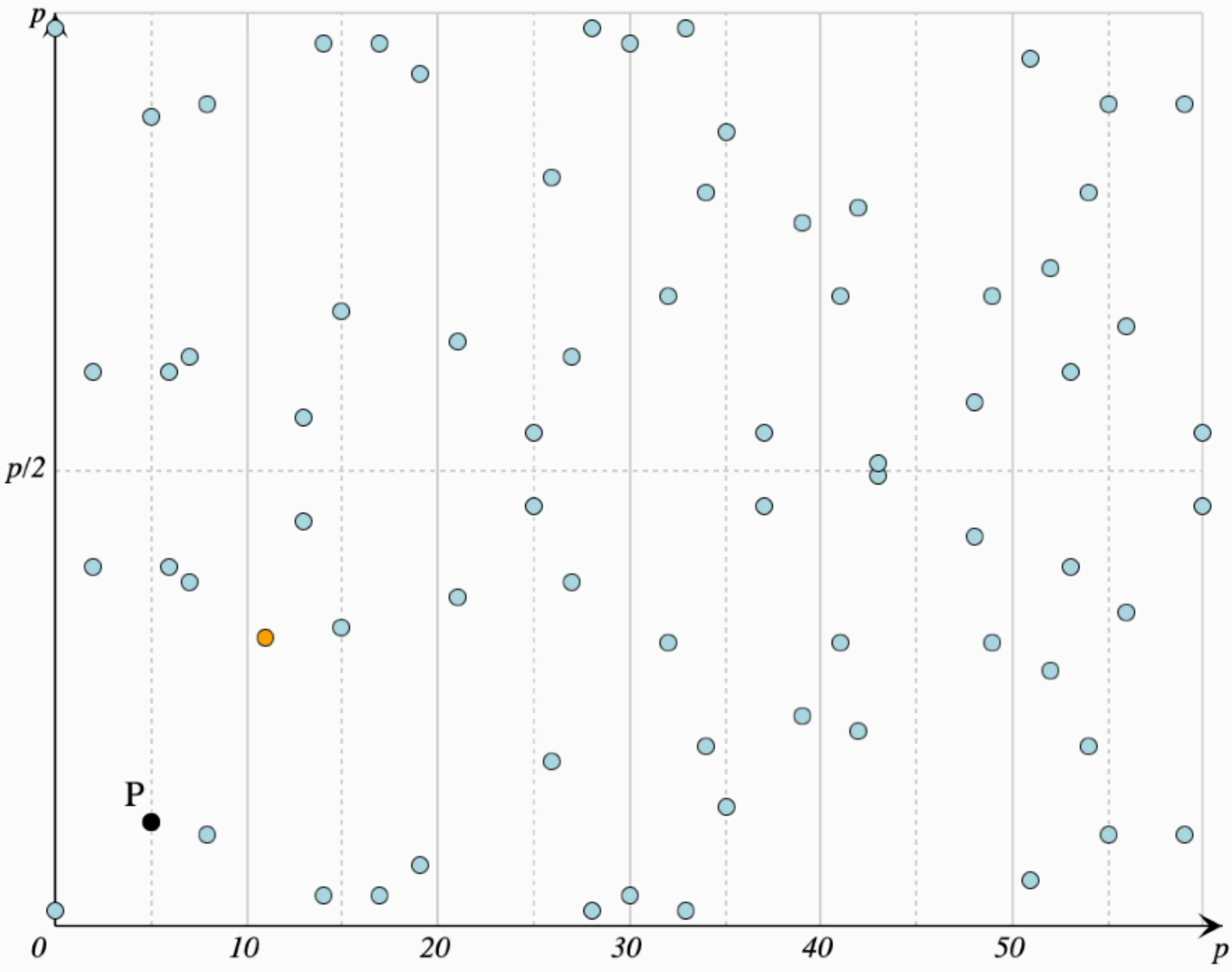


Doubling point repeatedly to find 2P through 128P

Double-and-add method for point 153P

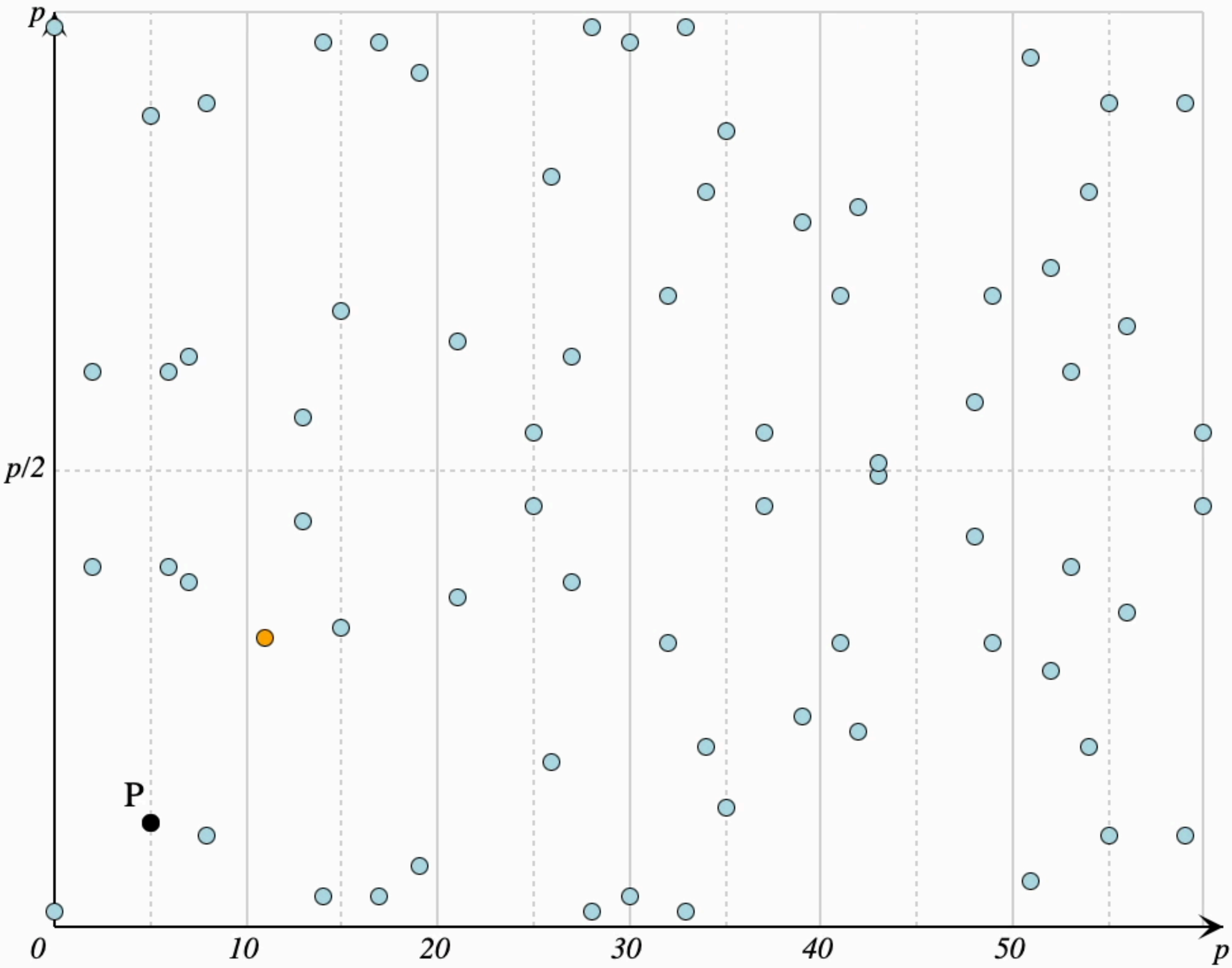
Addition et doublement

7



Doubling point repeatedly to find 2P through 128P

Double-and-add method for point 153P



Doubling point repeatedly to find 2P through 128P

Double-and-add method for point 153P

Addition et doublement

(Aka *square and multiply*)

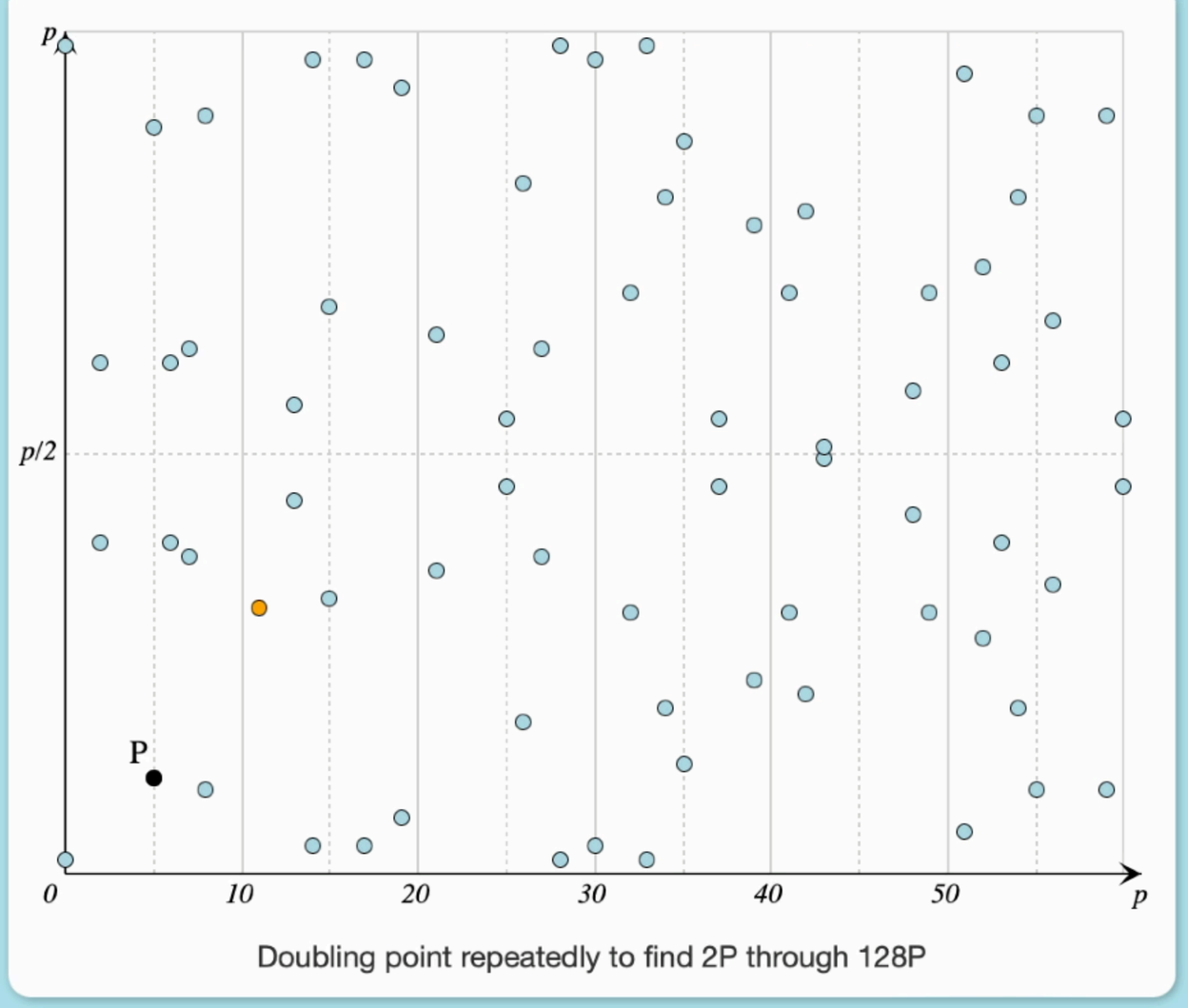
- Doubler P à répétition

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

- 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

Logarithme discret

Problème difficile

- Sachant $n \in \mathbb{Z}$, calculer le point nP est rapide (par addition et doublement)
- Mais ayant le point $nP \in \mathscr{C}$, retrouver n est difficile (il faut énumérer)