- **Test de Miller-Rabin :**

Théorème. Soit la décomposition $\tilde{p} - 1 = 2^u \cdot r$ où r est impair. S'il $\exists\, a \in \mathbb{N}$,

$$a^r \not\equiv 1 \bmod \tilde{p} \quad \text{et} \quad a^{r \cdot 2^j} \not\equiv \tilde{p} - 1 \bmod \tilde{p}$$

$\forall j = \{0, \dots, u-1\}$, alors $\tilde{p}$ est composé. Sinon $\tilde{p}$ premier avec grde probabilité.

Exercice. Écrire un algorithme de test de primalité basé sur le théorème Miller-Rabin.