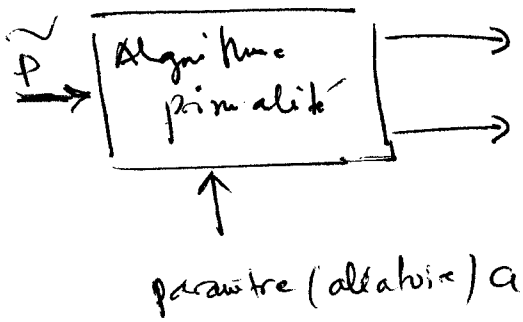
(Q1) $\mathbb{P}[\tilde{p} \text{ est premier}] \simeq \frac{2}{\ln(\tilde{p})}$.

Ex: RSA, module $n = 1024$ bits. $|p| = |q| \simeq \frac{1024}{2} = 512$.

$$\mathbb{P}(\tilde{p} \text{ premier}) \simeq \frac{2}{\ln(2^{512})} = \frac{2}{512 \cdot \ln 2} \cong \frac{1}{177}.$$

$\Rightarrow$ on teste 177 fois $\tilde{a}$ pour $\tilde{p}$ ☒

(Q2) Test de primalité est plus facile que la factorisation.



- Test de Fermat (basé sur le théorème de Fermat).

Entrée : $\tilde{p}$ candidat et λ (paramètre sécurité).

Sortie : $\tilde{p}$ composé ou $\tilde{p}$ est probablement premier.

1. Pour $i = 1$ à λ faire.
   - 1.1. choisir $a \in \{2, 3, \dots, \tilde{p} - 2\}$.
   - 1.2. Si $a^{\tilde{p}-1} \neq 1$.
   - 1.3. alors retourner ($\tilde{p}$ est composé).
2. Retourner ($\tilde{p}$ est premier avec une grande prob.).

(Théo. Fermat : si p premier, $a^{p-1} \equiv 1 \bmod p$).