TP8 : Primalité

Résumé du TP

Bertrand Meyer

27 avril 2022

Contexte

- Gros besoins industriels de nombres premiers.
- Test de primalité déterministes en temps polynomial mais non efficace.
- Tests probabilistes efficaces.
- Générer un nombre premier : cas classique de « chercher du foin dans une botte de foin ».

Rabin-Miller

Un test raté : Fermat

Théorème (Fermat)
Si p premier, alors $a^{p-1} = 1 \mod p$.

Raison
$\mathbb{F}_p^\times$ est un groupe cyclique d'ordre $p-1$.

Test de Fermat
S'il existe a premier avec n tel que $a^{n-1} \neq 1 \mod n$, alors n est composé.

Limite : il existe des entiers n qui ne sont jamais détectés par ce test.

Rafinement : Rabin-Miller

Proposition
Soit $2^v m$ la factorisation de $p-1$. Alors soit $a^m = 1 \mod p$ ou l'un des carrés successifs de a^m vaut -1.

Raison
Si p est premier, on passe par la suite de carrés

$$a^m;\ a^{2m};\ a^{4m};\ \dots;\ a^{p-1} = 1$$

Or dans un corps, il n'y a que ± 1 comme racines carrées de 1.

Test de Rabin-Miller
S'il existe a qui viole la proposition, n est composé.

Avantage : si n est composé, il y a au moins $\frac{3}{4}\varphi(n)$ témoins.

Solovay-Strassen

Solovay-Strassen

$$\text{Symbole de Legendre : } \left(\frac{a}{n}\right) = \begin{cases} 1 & \text{si } a \text{ est carré} \\ -1 & \text{si } a \text{ est non-carré} \end{cases}$$

(se calcule avec les règles de réciprocité quadratique).

Proposition

n (impair) est premier ssi pour tout a, $\left(\frac{a}{n}\right) = a^{(n-1)/2} \mod n$

Test de Solovay-Strassen

S'il existe a qui viole la proposition, n est composé.

Avantage : si n est composé, il y a au moins $\frac{1}{2}\varphi(n)$ témoins.