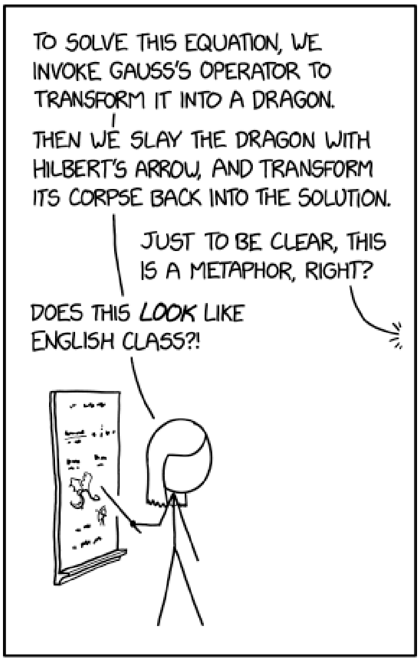
MPI* Info

Tests de primalité probabilistes

- TD9 -



ALL ADVANCED MATH TECHNIQUES

Clément Saulgeot

1 Test de Fermat

Question 1.

Démonstration d'Euler et de Leibniz

Soit n premier, montrons par récurrence sur $a \in \{1, ..., n-1\}$ que $a^n \equiv a[n]$.

Initialisation : Si a = 1, alors c'est évident.

Hérédité : Supposons l'hypothèse de récurrence vérifiée au rang $a \in \{1, ..., n-2\}$ et montrons qu'elle reste vraie au rang $a+1$.

$$\begin{aligned}(a+1)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k \\ &= a^n + 1 + \sum_{k=1}^{n-1} \binom{n}{k} a^k\end{aligned}$$

Il suffit alors de remarquer que $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$ pour tout $k \in \{1, ..., n-1\}$. Dès lors, $\binom{n-1}{k-1}$ et $\binom{n}{k}$ étant des entiers non nuls et k étant premier avec n (car n premier), on en déduit par théorème de gauß que k divise $\binom{n-1}{k-1}$. Ainsi, la somme est multiple de n.

$$\begin{aligned}(a+1)^n &\equiv a^n + 1[n] \\ &\equiv a + 1[n] \qquad \text{par hypothèse de récurrence}\end{aligned}$$

Conclusion : Ainsi, $a(a^{n-1} - 1) \equiv 0[n]$ et a étant inversible dans $\mathbb{Z}/n\mathbb{Z}$, car a est premier avec n, $a^{n-1} - 1 \equiv 0[n]$. D'où le résultat souhaité.

Démonstration par le théorème de Lagrange

Théorème de Lagrange

Pour tout groupe fini G et tout sous-groupe H de G, l'ordre de H divise celui de G : |H| divise |G|.
(Rappel : l'ordre d'un groupe fini est son nombre d'éléments.)

Le groupe engendré par l'élément a dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est de cardinal O(a).
Par définition de l'ordre, $a^{O(a)} \equiv 1[n]$.
Par théorème de Lagrange, $O(a) \mid |(\mathbb{Z}/n\mathbb{Z})^*|$.
Comme $|(\mathbb{Z}/n\mathbb{Z})^*| = n-1$, on peut passer la congruence à la puissance entière $\frac{n-1}{O(a)}$ et obtenir le résultat souhaité.

Question 2.

```c
int expo_modulaire(int x, int n, int p){
    //Precondition : p >= 1 et n >=1
    if(n == 1){
        return x%p;
    }
    int rec = expo_modulaire(x,n/2,p);
    if(n%2 == 0){
        return (rec*rec)%p;
    }
    else{
        return (rec*rec*x)%p;
    }
}
```

En notant $C(n)$ le nombre de multiplications effectuées, $C(n) = C(n/2) + O(1)$, d'où $C(n) = O(log_2(n))$.

Question 3.

```c
bool est_premier_fermat(int p){
    int x = (rand()%(p-1))+1;
    return (expo_modulaire(x,p-1,p) == 1);
}
```

Question 4.
Si $\{a \in \{1,\dots,n-1\}, a^{n-1} \equiv 1[n]\} = A$ est un sous groupe de $\mathbb{Z}/n\mathbb{Z}$, alors, d'après le théorème de Lagrange rappelé plus haut, $|A| \mid |\mathbb{Z}/n\mathbb{Z}|$.
Comme les deux groupes sont distincts (n n'est pas un nombre de Carmichael) : $|A| \leq \frac{|\mathbb{Z}/n\mathbb{Z}|}{2}$
Ainsi, P(erreur) = $\frac{|A|}{|\mathbb{Z}/n\mathbb{Z}|} \leq \frac{1}{2}$ par équiprobabilité.

Question 5.
On cherche d, le nombre d'appels minimaux à la fonction est_premier_fermat. Alors, $\frac{1}{2^d} \leq 10^{-20} \leq \frac{1}{2^{d-1}}$. La résolution nous donne d = 67.

On implémente donc la fonction suivante :

```c
bool est_presque_premier_fermat(int p){
    for (int i = 0 ; i < 67 ; i+=1){
        if (!est_premier_fermat(p)){
            return false;
        }
    }
    return true;
}
```

2 Test de Miller Rabin

Question 1. On rappelle la propriété suivante

Proposition

Si n est premier, alors $((\mathbb{Z}/n\mathbb{Z})^*, *)$ est un corps.

Ainsi, on cherche les éléments $x \in (\mathbb{Z}/n\mathbb{Z})^*$ tels que $\overline{x^2} = \overline{1}$. Or, soit $x \in (\mathbb{Z}/n\mathbb{Z})^*$, on a

$$\begin{aligned} \overline{x^2} = \overline{1} &\Leftrightarrow \overline{x^2 - 1} = \overline{0} \\ &\Leftrightarrow \overline{(x+1)(x+1)} = \overline{0} \end{aligned}$$

Et comme $((\mathbb{Z}/n\mathbb{Z})^*, *)$ est un corps, on peut dire que

$$\overline{x^2} = \overline{1} \Leftrightarrow \begin{cases} \overline{(x+1)} & = \overline{0} \\ \textbf{ou} & \\ \overline{(x-1)} & = \overline{0} \end{cases}$$

Les seules solutions possibles sont donc $x = \pm 1$

Question 2.

Soit $a \in [\![1; n-1]\!]$. Supposons que la condition (1) n'est pas vérifiée.
Alors, $a^m \not\equiv 1[n]$ et on sait, d'après le petit théorème de Fermat, que $a^{n-1} \equiv 1[n]$.
Ainsi, $a^{2^0 \times m} \not\equiv 1[n]$ et $a^{2^s \times m} \equiv 1[n]$. Il existe donc $d \in [\![0; s-1]\!]$ tel que pour tout $j \in [\![0; d]\!]$ $a^{2^j \times m} \not\equiv 1[n]$ et $a^{2^{d+1} \times m} \equiv 1[n]$.
Dès lors, d'après la question 1, $a^{2^d \times m} \equiv -1[n]$ ou $a^{2^d \times m} \equiv 1[n]$, ce qui est exclu.
Donc (2) est vérifiée pour d.

Question 3.

$\boxed{a}$ $t^n = (1 + nq^{e-1})^n = 1 + nq^{e-1} + \sum_{k=2}^{n} \binom{n}{k} q^{k(e-1)}$
$q^{k(e-1)} = q^e q^{k(e-1)-e}$
Comme $k \geq 2$, $k(e-1) - e \geq 2(e-1) - e = e - 2$. Comme $e \geq 2$, on en déduit que $k(e-1) - e \geq 0$.
Ainsi, $q^e q^{k(e-1)-e} = nq^{k(e-1)-e}$ avec $q^{k(e-1)-e}$ entier pour tout k de la somme.
Finalement, $t^n \equiv 1[n]$.

$\boxed{b}$ Il suffit de voir que si $t^{n-1} \equiv 1[n]$, $t^n \equiv t \equiv 1[n]$.
Alors, $q^{e-1} \equiv 0[q^e]$. Or, $0 < q^{e-1} < q^e$, donc c'est absurde.

$\boxed{c}$ Supposons que d convienne. Alors $d^{n-1} \equiv 1[n]$.
Et $(dt)^{n-1} \equiv d^{n-1} t^{n-1} \equiv t^{n-1} \not\equiv 1[n]$
Pour montrer que les dt sont distincts, par contraposée :
$d_1 t \equiv d_2 t[n] \Rightarrow d_1 t^n \equiv d_2 t^n [n] \Rightarrow d_1 \equiv d_2[n]$ d'après a.

$\boxed{d}$ Il y a au moins autant de a avec lequel n ne passe pas le test de Fermat que de a avec lequel il le passe, car pour chaque a qui convient, at [n] ne convient pas, et ces at [n] sont distincts deux à deux. Dès lors, P(erreur au test de Fermat) $\leq \frac{1}{2}$ et P(n ne passe pas le test de Fermat pour a ou a est un témoin de Miller Rabin pour n) $\geq \frac{1}{2}$ avec le n choisit.

Question 4.

1 est un co-témoin qui satisfait (1) et (n-1) est un co-témoin qui satisfait (2) pour d = 0 car $n - 1 \equiv -1[n]$ et m étant impair, $(-1)^{2^0 m} \equiv -1[n]$.

Question 5.

D'après la décomposition en facteurs premiers, n n'était pas premier ni de la forme q^e avec q premier, il existe au moins 2 nombres premiers différents apparaissant dans la décomposition. Ainsi, on peut découper n en produit de deux nombres premiers entre eux.

Question 6.

$\boxed{a}$ D'après le théorème des restes chinois (V.2), il existe un unique $t \in [\![0; n-1]\!]$ tel que $t \equiv h[q]$ et $t \equiv 1[r]$.

$\boxed{b}$ Par définition, $t^{2^d m} \equiv h^{2^d m} \equiv -1[n]$ donc $t^{2^d m} \equiv -1[q]$ car $n = qr$.
La deuxième congruence est évidente à montrer.

$\boxed{c}$ Supposons que $t^m \equiv 1[n]$. Alors $t^m \equiv 1[q]$ donc $t^{2^d m} \equiv 1[q]$. Ce qui est absurde d'après b.
Donc t ne vérifie pas (1).
Supposons qu'il existe $i \in \{0,...,s-1\}$ tel que $t^{2^i m} \equiv -1[n]$.
Alors $t^{2^i m} \equiv -1[q]$ et $t^{2^i m} \equiv -1[r]$.
Comme d satisfait la propriété (2) de manière maximale, $i \leq d$. D'après b, $t^{2^d m} \equiv 1[r]$, donc $i < d$. Or, si $i < d$, $t^{2^d m} \equiv 1[r]$ et $t^{2^d m} \equiv 1[q]$, donc $t^{2^d m} \equiv 1[n]$, ce qui est absurde par maximalité de d.
Ainsi, t ne vérifie pas (2). Dès lors, t est un témoin de Miller-Rabin pour n.

$\boxed{d}$ Soit d un co-témoin de Miller-Rabin.
<u>Si $d^m \equiv 1[n]$.</u>
Alors $(dt)^m \equiv t^m \not\equiv 1[n]$ et pour tout $i \in [\![0;s-1]\!]$, $(dt)^{2^i m} \equiv t^{2^i m} \not\equiv -1[n]$ (car $d^{2^i m} \equiv (d^m)^{2^i} \equiv 1[n]$ par hypothèse). Ainsi, dt est un témoin.
<u>S'il existe i_0 tel que $d^{2^{i_0} m} \equiv -1[n]$.</u>
Supposons que $(dt)^m \equiv 1[n]$. Alors $(dt)^{2^{i_0} m} \equiv 1[n]$, d'où $t^{2^{i_0} m} \equiv -1[n]$. Cela est absurde.
Supposons qu'il existe j_0 tel que $(dt)^{2^{j_0} m} \equiv -1[n]$.
Si $j_0 > i_0$, alors $t^{2^{j_0} m} \equiv -1[n]$, ce qui est absurde.
Si $j_0 = i_0$, $t^{2^{j_0} m} \equiv 1[n]$, d'où soit $t^m \equiv 1[n]$, soit il existe un rang $k < i_0$ tel que $t^{2^k m} \equiv -1[n]$ (démonstration identique qu'à la question 2). Ce qui est absurde car t est témoin.
Si $j_0 < i_0$, $(dt)^{2^{i_0} m} \equiv 1[n]$, et par hypothèse sur i_0, $t^{2^{i_0} m} \equiv -1[n]$, ce qui est absurde.
Ainsi, dt est un témoin.

Dans tous les cas, dt est un témoin. Si $d_1 t \equiv d_2 t[n]$, comme $t^{2^{d+1} m} \equiv 1[n]$ (car $t^{2^{d+1} m} \equiv 1[q]$ et $[r]$ (d'après b), puis le théorème des restes chinois donne le résultat), t est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$ d'inverse $t^{2^{d+1} m-1}$. Donc $d_1 \equiv d_2[n]$.

$\boxed{e}$ Il y a au moins autant de témoins de Miller-Rabin que de co-témoins donc, en prenant un élément au hasard, on a au moins une chance sur deux de tomber sur un témoin.

Question 7.

Algorithm 1 Entrées : entier `n`, erreur `e`

Si n est pair :
    Renvoyer (n==2)
Sinon :
    Répéter un certain nombre de fois (selon l'erreur e) :
        Tirer $a \in [\![2; n-1]\!]$
        Si $a^{n-1} \not\equiv 1[n]$:
            Renvoyer faux
        Calculer $n-1 = 2^s m$ avec m impair
        Si $a^m \not\equiv 1[n]$:
            $d \leftarrow 0$
            $p \leftarrow a^m$
            Tant que $d < s$ et $p \not\equiv -1[n]$:
                $d \leftarrow d+1$
                $p \leftarrow p^2$
                Si $d = s$
                    renvoyer faux
                Fin Si
            Fin Tant que
        Fin Si
    Fin Répéter
Fin Sinon
renvoyer vrai