TD - tests de primalité probabiliste

①

1. Soit n premier, on montre par récurrence sur $a \in \mathbb{N}$ que $a^n \equiv a \ [n]$

$a = 0$, $a = 1$ ok.

$$(a+1)^n = a^n + 1 + \underbrace{\sum_{k=1}^{n-1} \binom{n}{k} a^k}_{\text{divisible par } n \text{ qui est premier.}}$$

$$\equiv a^n + 1 \ [n]$$

$$\equiv a + 1 \ [n] \quad (HR)$$

Ainsi $a(a^{n-1} - 1) \equiv 0 \ [n]$ or a est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$ $(a \wedge n = 1)$ donc $a^{n-1} \equiv 1 \ [n]$.

↳ On peut aussi voir ce résultat comme un corollaire du thm de Lagrange appliqué au groupe $((\mathbb{Z}/n\mathbb{Z})^*, *)$ de cardinal $n-1$.

2.
```
int expo_mod(int x, int n, int p) {
    if (x==0) return 1;
    else {
        int v = expo_mod(x, n/2, p);
        if (n%2 == 0)
            return ((v*v)%p);
        else
            return((v*v*x)%p);
    }
```

Si on note C_n, le nombre de multiplications modulaires effectuées alors

$$C_n = C_{\frac{n}{2}} + O(1) \quad \Rightarrow C_n = O(\log_2(n))$$

3. On tire a au hasard dans $[\![2, n-1]\!]$ et on décide que n est premier si $a^{n-1} \equiv 1 \mod n$.

```
bool est_premie_fermat (int n) {
    int a = (rand() % (n-1)) + 1;
    return (expo_mod (a, n-1, n) == 1);
}
```

4. Si n n'est pas un nb de Carmichael alors

$G = \{a \in \{1, \dots, n-1\} : a^{n-1} \equiv 1 \ [n]\}$ est un ss gpe de $((\mathbb{Z}/n\mathbb{Z})^*, *)$ de cardinal $\varphi(n)$.

Ainsi $\#G \leq \varphi(n) \leq \frac{n-1}{2}$

↑ ss gpe strict dont le cardinal divise le cardinal total.

Ainsi

$$\text{Pr}(\text{erreur}) \leq \frac{\overbrace{\frac{n-1}{2} - 1}^{\#(G \setminus \{1\})}}{n-2} = \frac{n-3}{2(n-2)} \leq \frac{1}{2}.$$

5. Si on répète k fois, on obtient une erreur $\leq \frac{1}{2^k} \leq \frac{1}{10^{20}}$ ssi $10^{20} \leq 2^k$

ssi $20 \log 10 \leq k \log 2$

ssi $\frac{20 \log 10}{\log 2} \leq k$

ssi $67 \leq k$

On obtient donc le code suivant :

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

Si n est premier alors tous les 67 tests renverront vrais et on renverra vrai de manière certaine.
Si n n'est pas premier alors à chaque tour, la proba de renvoyer vrai est $\leq \frac{1}{2}$ et ainsi les appels étant II, la proba de renvoyer vrai à chaque fois $\leq \frac{1}{2^{67}} \leq \frac{1}{10^{20}}$

(2) 1. Si n est premier alors $\left((\mathbb{Z}/n\mathbb{Z})^*, *\right)$ est un corps donc l'équat° $X^2 - 1$ admet exactement deux solutions qui sont 1 et -1 d'après le thm de Gauss.

Ainsi 1 n'admet que 1 et -1 ĉ racines carrées.

2. On sait que $a^{n-1} \equiv 1 \ [n]$

Soit $\{a^{2^j \times m} \ ; \ 0 \leq j \leq d\}$

si $a^m \equiv 1 \ [n]$ alors (1) est vérifiée

sinon $a^{2^j \times m} \not\equiv 1 \ [n]$ et

$a^{2^d \times m} = a^{n-1} \equiv 1 \ [n]$

Soit j_0 le plus grd indice t.q $a^{2^{j_0} \times m} \not\equiv 1 \ [n]$ on a alors $a^{2^{j_0+1} \times m} = \left(a^{2^{j_0} \times m}\right)^2 \equiv 1 \ [n]$

et ainsi $a^{2^{j_0} \times m} \equiv -1$ ou 1 exclu $[n]$

Ainsi (2) est vérifiée.

3. (a) $t^n = \left(1 + q^{e-1}\right)^n = 1 + n q^{e-1} + \sum_{k=2}^{n} \binom{n}{k} q^{k(e-1)}$

or $q^{k(e-1)} = q^{e} \, q^{\overbrace{(k(e-1)-e}^{\geq 0}}$

$= q^e \, q^{\cdots} \equiv 0 \ [q^e]$

car $k(e-1) \geq e$ en effet pour $e=2$ on a bien $2 \leq k$

$\forall e \geq 3 \quad e \leq e+1 \leq 2(e-1) \leq k(e-1)$

$(k \geq 2 \text{ et } e > 1)$

$1 \leq k e - 2 \ (\Rightarrow e \geq 3$

(b) Si $t^{n-1} \equiv 1 [n]$ alors $t^n \equiv t \not\equiv 1 [n]$ ($q \not\equiv 0 [n]$ car $q < n$)

ce qui est contradictoire avec (a)

(c)
$$(dt)^{n-1} = d^{n-1} t^{n-1} \equiv t^{n-1} [n] \not\equiv 1 [n].$$

$d_1 t \equiv d_2 t [n] \Rightarrow d_1 \equiv d_2 [n]$ car puisque $t^n \equiv 1 [n]$ donc il suffit de multiplier par t^{n-1} de part et d'autre pour obtenir le résultat souhaité.

(d) Il y a au $\ominus$ autant de a avec lequel n ne passe pas le test de Fermat que de a avec lequel il le passe ainsi dans ce cas on sait que la proba d'erreur du test de Fermat est $\leq \frac{1}{2}$.

4. 1 est un cotemoin de type 1 et (-1) de type(2) avec $d = 0$ car n est impair donc $(-1)^n \equiv -1$

5. Thm de factorisat° des nbs entiers naturels → il y a au $\ominus$ 2 nbs 1ers apparaissant dans la factorisation ce qui permet de la découper en deux produits non triviaux premiers entre eux.

6. (a) thm Chinois avec q et r premiers entre eux

(b) $t^{2^d \times m} = h^{2^d \times m} \equiv -1 \bmod q$ (**)

$t^{2^d \times m} \equiv 1 \bmod r$

(c) (1) n'est pas vérifiée car sinon
$t^{2^d \times m} \equiv 1 \bmod n \Rightarrow t^{2^d \times m} \equiv 1 \bmod q$

Si (2) est vérifiée alors $\exists d'$ t q
$t^{2^{d'} \times m} \equiv -1 \bmod n$ et donc
(*) $t^{2^{d'} \times m} \equiv -1 \bmod$ ~~q~~ or ~~b~~ (or impair $\Rightarrow 1 \neq -1$)

Or $d' \leq d$ par maximalité de d
donc et (*) garantit que $d' \neq d$ i.e
$d' < d$.

Mais dans ce cas, on aurait
$t^{2^i \times m} \equiv 1 \bmod n \ \forall i > d'$ en
particulier pour $i = d$ ce qui
est exclu par (**)

On en déduit bien que t est un
témoin de Miller Rabin pour n.

(d) ~~$(t^d)^m = t^m$ [n]~~

Soit d un co-témoin de Miller Rabin,

↳ Si $d^m = 1\ [n]$ alors $(dt)^m \equiv t \not\equiv 1\ [n]$

et $\forall j \in [\![0, s-1]\!]$, $(dt)^{2^j \times m} \equiv t^{2^j \times m} \not\equiv 1\ [n]$

↳ Si $\exists j_0$ t.q $d^{2^{j_0} \times m} \equiv -1\ [n]$ alors $j_0 \leq d$ par définition et pour tout co-témoin x, on aura $x^{2^{d+1} \times m} \equiv 1\ [n]$ et $x^{2^d \times m} \equiv \pm 1\ [n]$

or $(dt)^{2^d \times m} \equiv \pm \underbrace{t^{2^d \times m}}_{\not\equiv -1 \text{ et } \not\equiv 1 \text{ par } (**)}$

donc $(dt)^{2^d \times m} \not\equiv \pm 1\ [n]$ ce qui exclu la possibilité que ce soit un co-témoin, c'est donc un témoin.

$d_1 t \equiv d_2 t\ [n] \Rightarrow d_1 \equiv d_2\ [n]$ car

$t^{m \times 2^{d+1}} \equiv 1 \mod [n]$ ($\equiv 1 \mod q$ et mod r donc par thm Chinois (unicité))

donc t est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$ d'inverse $t^{\frac{m \times 2^{d+1}}{n} - 1}$

(e) Il y a autant ⊖ de témoins de Miller Rabin que de co-témoins donc si on prend un dt au hasard on a autant ⊖ une chance sur 2 de tomber sur un témoin.

7. Algo entrée n.

1) Si n est pair, renvoyer vrai ssi $n=2$.

Un certain nb de fois (suivant l'erreur)

2) Tirer $a \in \{2, \dots, n-1\}$

(a) si $a^{n-1} \neq 1 \ [n]$
renvoyer faux

(b) calculer $n-1 = m \times 2^s$ avec m impair

(c) si $a^m \equiv 1 \ [n]$ ne rien faire càd ~~renvoyer vrai~~ retourner en 2)

(d) sinon $d \leftarrow 0 \quad p \leftarrow a^m$
while $(d < s \ \& \ p \neq 1 \ [n])$
d++
$p \leftarrow p * p$

si $d = s$
renvoyer faux

~~renvoyer vrai~~

3) Renvoyer vrai

On sait que si n est premier alors pour tout a, il passera le test (a) puis le test (c) ou le (d) sans renvoyer faux. Si n est composé pair, on renverra faux par 1) et sinon on a à chaque tour une proba au $\ominus$ $1/2$ de tirer a qui permettra de renvoyer faux