Théorie des Nombres - TD4
Tests de primalité

Exercice 1 : (Test de Fermat et nombres de Carmichael)
Soit $n \in \mathbb{N}$, $n \geq 2$.

a) Montrer que si n est premier, alors pour tout entier a premier à n, $a^{n-1} \equiv 1\ [n]$. En déduire un test de non-primalité et estimer sa complexité.

b) Soient p, q premiers distincts tels que $\text{pgcd}(p-1, q-1) = 2$ et $n = pq$. Montrer que 2^{n-1} n'est pas congru à 1 modulo n. Généraliser au cas où l'entier $d := \text{pgcd}(p-1, q-1)$ vérifie $2^d \leq n$.

c) L'entier $n \geq 2$ est appelé nombre de Carmichael si n n'est pas premier et si pour tout entier a premier à n, $a^{n-1} \equiv 1\ [n]$.

i) Montrer que n est un nombre de Carmichael si et seulement si n est impair, sans facteur multiple, et pour tout premier p divisant n, $p-1$ divise $n-1$.

ii) Montrer que pour $m \geq 1$, si $6m+1$, $12m+1$ et $18m+1$ sont premiers, alors $(6m+1)(12m+1)(18m+1)$ est de Carmichael. En déduire un exemple de nombre de Carmichael.

iii) Montrer qu'un nombre de Carmichael a au moins trois facteurs premiers.

iv) Soit r un entier premier impair. Montrer qu'il n'existe qu'un nombre fini de nombres de Carmichael de la forme pqr, avec p, q premiers.

[On pourra montrer que $p-1$ divise $rq-1$ et $q-1$ divise $rp-1$, puis majorer le nombre $\frac{qr-1}{p-1}\frac{pr-1}{q-1}$.]

v) Déterminer tous les nombres de Carmichael admettant exactement trois facteurs premiers, dont l'un vaut 3 (resp. 5, resp. 7).

Solution de l'exercice 1.

a) C'est le petit théorème de Fermat. On dispose donc du test de non-primalité suivant pour l'entier n : choisir $a \in \mathbb{Z}$ premier à n, puis tester si $a^{n-1} \equiv 1\ [n]$. Si ce n'est pas le cas, alors n n'est pas premier. La complexité de ce test est la suivante : pour a fixé, on doit calculer a^{n-1} modulo n, ce qui se fait via une exponentiation modulaire rapide, d'où une complexité en $\mathcal{O}(\log(n)^3)$ opérations élémentaires.

b) On traite directement le cas général, sous l'hypothèse $2^d \leq n$. Supposons que $2^{n-1} \equiv 1\ [n]$. Alors $2^{pq-1} \equiv 1\ [p]$ et $2^{pq-1} \equiv 1\ [q]$, donc $2^{q-1} \equiv 1\ [p]$ et $2^{p-1} \equiv 1\ [q]$ (puisque $2^{p-1} \equiv 1\ [p]$ et $2^{q-1} \equiv 1\ [q]$). Donc l'ordre de 2 modulo p (resp. modulo q) divise $p-1$ et $q-1$, donc divise d. Donc $2^d \equiv 1\ [p]$ et $2^d \equiv 1\ [q]$, i.e. $2^d \equiv 1\ [n]$. Or $2^d \leq n$ par hypothèse, donc $2^d = 1$, donc $d = 0$, ce qui est impossible. Donc finalement 2^{n-1} n'est pas congru à 1 modulo n.

c) i) – On suppose que n est un nombre de Carmichael. En appliquant la définition à $a = -1$, on obtient que $(-1)^{n-1} \equiv 1\ [n]$, donc $(-1)^{n-1} = 1$, donc n est impair. Supposons qu'il existe un nombre premier p tel que p^2 divise n. Alors le lemme chinois et la structure de $(\mathbb{Z}/p^r\mathbb{Z})^*$ (avec $r \geq 2$) assure que $(\mathbb{Z}/n\mathbb{Z})^*$ admet un élément a d'ordre p, donc puisque $a^{n-1} \equiv 1\ [n]$, p divise $n-1$. Or p divise n, d'où une contradiction. Donc finalement n est sans facteur carré. Soit p premier divisant n. Montrons que $p-1$ divise $n-1$. Le lemme chinois assure que le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ admet un facteur direct $(\mathbb{Z}/p\mathbb{Z})^*$, qui est cyclique d'ordre $p-1$. Donc il existe un élément x d'ordre $p-1$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Puisque $x^{n-1} \equiv 1\ [n]$, cela assure que $p-1$ divise $n-1$.

– Montrons la réciproque. On suppose n impair, sans facteur multiple, tel que pour tout p premier divisant n, $p-1$ divise $n-1$. Soit $a \in \mathbb{Z}$ premier à n. Soit p premier divisant n. Puisque $p-1$ divise $n-1$, et a étant premier à p, on a $a^{n-1} \equiv 1\ [p]$. Ceci étant valable pour tout p premier divisant n et n étant sans facteur carré, le lemme chinois assure que $a^{n-1} \equiv 1\ [n]$, ce qui conclut la preuve.

ii) On note $n = (6m+1)(12m+1)(18m+1)$. Par la question précédente, il suffit de vérifier que $6m$, $12m$ et $18m$ divisent $n-1$. Or on a $n \equiv 1.1.1 \equiv 1\ [6m]$, $n \equiv (6m+1).1.(6m+1) \equiv 1+12m+36m^2 \equiv 1\ [12m]$ et $n \equiv (6m+1)(-6m+1).1 \equiv 1-36m^2 \equiv 1\ [18m]$, ce qui assure que n est de Carmichael.

On constate que pour $m = 1$, les nombres 7, 13 et 19 sont premiers. Par conséquent, le nombre $n = 7.13.19 = 1729$ est un nombre de Carmichael.

De même, pour $m = 6$, on obtient les nombres premiers 37, 73 et 109, donc l'entier $n = 37.73.109 = 294409$ est un nombre de Carmichael.

iii) Soit $n = pq$ un nombre de Carmichael avec deux facteurs premiers impairs $p < q$. La question i) assure que $q-1$ divise $n-1$. Or $n-1 = p(q-1)+p-1$, donc $q-1$ divise $p-1$. Or $p < q$, donc ceci est contradictoire. Donc un nombre de Carmichael admet au moins trois facteurs premiers.

iv) La question i) assure que $p-1$ divise $pqr-1 = qr(p-1)+qr-1$, donc $p-1$ divise $qr-1$. De même, $q-1$ divise $pr-1$. Il existe donc $a, b \in \mathbb{N}$, $a, b \geq 2$, tels que $qr-1 = a(p-1)$ et $pr-1 = b(q-1)$. On en déduit que $p = \frac{r(b-1)+b(a-1)}{ab-r^2}$ et $q = \frac{1+a(p-1)}{r}$. En particulier, les valeurs de a et b déterminent p et q. Il suffit donc de montrer qu'il n'y a qu'un nombre fini de valeurs possibles pour a et b.

Pour cela, on considère le produit $ab = \frac{qr-1}{p-1}\frac{pr-1}{q-1} = \frac{pr-1}{p-1}\frac{qr-1}{q-1}$. Si on note f_r la fonction définie sur $]1;+\infty[$ par $f_r(x) = \frac{rx-1}{x-1}$, on voit facilement que f_r est strictement décroissante et tend vers r^2 en $+\infty$. Cela assure que pour tous p, q premiers impairs distincts, on a $r^2 < ab \leq f_r(3)f_r(5)$. Or il est clair que ces inégalités ne sont satisfaites que par un nombre fini d'entiers $a, b \geq 2$. Donc il n'existe qu'un nombre fini de premiers p, q tels que pqr soit un nombre de Carmichael.

v) – On fixe $r = 3$ dans la question précédente. Avec les notations de cette question, on obtient $9 = r^2 < ab \leq f_3(5)f_3(7)$, i.e. $10 \leq ab \leq 11$ avec $a, b \geq 2$ entiers. Quitte à échanger a et b (ce qui revient à échanger p et q), on peut supposer $a \leq b$. Donc $ab = 10$, donc $(a;b) = (2;5)$. On en déduit via les formules de la question iv) que $p = 17$ et $q = 11$. Par conséquent, il existe un unique nombre de Carmichael à trois facteurs premiers qui soit divisible par 3, c'est $3.11.17 = 561$. C'est le plus petit nombre de Carmichael.

– On fixe $r = 5$ dans la question iv). Avec les notations de cette question, on obtient $25 = r^2 < ab \leq f_5(7)f_5(11)$, i.e. $26 \leq ab \leq 30$ avec $a, b \geq 2$ entiers. Quitte à échanger a et b, on peut supposer $a \leq b$. Donc $ab = 26, 27, 28, 29$ ou 30, donc $(a;b) \in \{(2;13), (2;14), (2;15), (3;9), (3;10), (4;7), (5;6)\}$. On en déduit via les formules de la question iv) que $(p,q) \in \{(17;13), (29;17), (73;29)\}$. Par conséquent, il existe trois nombres de Carmichael à trois facteurs premiers qui soient divisibles par 5, ce sont $5.13.17 = 1105$, $5.17.29 = 2465$ et $5.29.73 = 10585$.

– On fixe $r = 7$ dans la question iv). Avec les notations de cette question, on obtient $49 = r^2 < ab \leq f_7(11)f_7(13)$, i.e. $50 \leq ab \leq 57$ avec $a, b \geq 2$ entiers. Quitte à échanger a et b, on peut supposer $a \leq b$. Donc $ab = 50, 51, 52, 53, 54, 55, 56$ ou 57, donc

$$(a;b) \in \{(2;25), (2;26), (2;27), (2;28), (3;17), (3;18), (3;19), (4;13), (4;16), (5;10), (5;11), (6;9), (7;8)\}.$$

On en déduit via les formules de la question iv) que

$$(p,q) \in \{(19;13), (31;13), (41;23), (67;19), (73;31), (103;73)\}.$$

Par conséquent, il existe six nombres de Carmichael à trois facteurs premiers qui soient divisibles par 7, ce sont $7.13.19 = 1729$, $7.13.31 = 2821$, $7.19.67 = 8911$, $7.23.41 = 6601$, $7.31.73 = 15841$ et $7.73.103 = 52633$.

Exercice 2 : (Test de Solovay-Strassen)

a) Montrer que si n est premier, alors $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]$ pour tout entier a premier à n.

b) Soit $n > 2$ impair. On suppose que $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]$ pour tout entier a premier à n. Montrer que n est premier.
[Indication : on pourra utiliser l'exercice 1 et la caractérisation des nombres de Carmichael.]

c) En déduire un test de non-primalité et évaluer sa complexité.

d) Montrer que si n est impair composé, alors le nombre d'entiers $1 \leq a < n$ premiers à n tels que $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]$ est inférieur ou égal à $\frac{\varphi(n)}{2}$.

e) En déduire un test de primalité probabiliste et évaluer son efficacité.

Solution de l'exercice 2.

a) cf cours.

b) En élevant au carré la relation $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]$, on obtient que n est soit un nombre premier, soit un nombre de Catalan. Donc n est produit de facteurs premiers impairs deux-à-deux distincts. Supposons que n admette au moins deux facteurs premiers, dont l'un est noté p. Alors le lemme chinois assure qu'il existe $a \in \mathbb{Z}$, premier à n, tel que a ne soit pas un carré modulo p et a est congru à 1 modulo tous les facteurs premiers de n distincts de p. Alors $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) = -1$, et la classe de $a^{\frac{n-1}{2}}$ modulo n vaut 1 modulo tout facteur premier de n distinct de p. Donc le lemme chinois assure que $a^{\frac{n-1}{2}}$ n'est pas congru à -1 modulo n, ce qui contredit l'hypothèse. Donc n est premier.

c) On dispose du test suivant : pour a premier à n fixé, on teste si $a^{\frac{n-1}{2}}$ est congru à $\left(\frac{a}{n}\right)$ modulo n. Si ce n'est pas le cas, alors n n'est pas premier. Le calcul de $a^{\frac{n-1}{2}}$ modulo n a une complexité en $\mathcal{O}(\log(n)^3)$, et la loi de réciprocité quadratique assure que la complexité du calcul du symbole de Jacobi $\left(\frac{a}{n}\right)$ est également en $\mathcal{O}(\log(n)^3)$. D'où finalement un test de non-primalité (à a fixé) en $\mathcal{O}(\log(n)^3)$.

d) Soit n impair composé. On note $H_n := \{1 \leq 1 < n : \text{pgcd}(a,n) = 1 \text{ et } \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]\}$. Alors la multiplicativité du symbole de Jacobi et de l'élévation à la puissance $\frac{n-1}{2}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ assure que H_n est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$ (H_n contient clairement la classe de 1). En outre, puisque n est composé, la question b) assure que H_n n'est pas le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ tout entier, par conséquent, on a $\#H_n \leq \frac{\varphi(n)}{2}$. Cela répond à la question posée.

e) On fixe un entier $k \geq 1$. On tire au hasard (disons uniformément) un entier $1 \leq a_1 < n$ premier à n, et on teste si $a_1^{\frac{n-1}{2}}$ est congru à $\left(\frac{a_1}{n}\right)$ modulo n. Puis on tire un entier $1 \leq a_2 < n$ premier à n (indépendant de a_1 par exemple), et on recommence k fois. On fait donc k tirages aléatoires indépendants $(a_1, \ldots, a_n)$, de loi uniforme, parmi les entiers entre 1 et $n-1$, premiers à n. Si pour l'un des a_i, la réponse est négative, alors on peut conclure que le nombre n est composé. Si toutes les réponses sont positives, on ne peut pas conclure avec certitude que n est premier. En revanche, on dit parfois que n est probablement premier (ou pseudo-premier) : la probabilité que n que ne soit pas premier est en effet inférieure à $\frac{1}{2^k}$ d'après la question d). La complexité de cet algorithme est $\mathcal{O}(k.\log(n)^3)$. Évidemment, plus k est grand, plus la complexité est élevée et plus le risque d'erreur est faible.

Exercice 3 : (Test de Miller-Rabin) Soit $n > 2$.

a) Montrer que si n est premier et $n-1 = 2^s t$ avec t impair, alors pour tout a premier à n, soit $a^t \equiv 1\ [n]$, soit il existe $0 \leq i < s$ tel que $a^{2^i t} \equiv -1\ [n]$. En déduire un test de non-primalité. et estimer sa complexité

b) On suppose n impair composé. Un entier a premier à n est appelé témoin de Miller pour n si la conclusion de la question précédente n'est pas vérifiée.

i) Montrer que 2 est un témoin de Miller pour 561.

ii) Soit G un groupe cyclique, soient $m \in \mathbb{Z}$, $g \in G$, $k := \text{pgcd}(m, \#G)$. Montrer que l'équation $x^m = g$ a une solution dans G si et seulement si $g^{\frac{\#G}{k}} = 1$. Montrer que dans ce cas, l'équation a exactement k solutions.

iii) Avec les notations précédentes, on suppose que g est d'ordre 2, on note $\#G = 2^u v$ (v impair) et $m = 2^s t$ (t impair). On pose $r := \min(u, s)$ et $w := \text{pgcd}(t, v)$.

i. Montrer que l'équation $x^t = 1$ a w solutions dans G.

ii. Montrer que si $1 \leq j \leq r$, l'équation $x^{2^{j-1}t} = g$ a $2^{j-1}w$ solutions dans G.

iii. Montrer que si $j > r$, l'équation $x^{2^{j-1}t} = g$ n'a pas de solution dans G.

iv. On revient aux notations initiales : $n \geq 2$, $n-1 = 2^s t$ avec t impair. On considère le groupe $G := (\mathbb{Z}/n\mathbb{Z})^*$ et les $s+1$ équations $x^t = 1$, $x^t = -1$, $x^{2t} = -1$, $\ldots$, $x^{2^{s-1}t} = -1$. On décompose $n = \prod_{i=1}^N p_i^{a_i}$ en facteurs premiers. On note aussi $p_i^{a_i - 1}(p_i - 1) = 2^{u_i} v_i$ avec v_i impair, $w_i := \text{pgcd}(t, v_i)$, $v_i' := \frac{v_i}{w_i}$, $U := \sum_i u_i$, $V := \prod_i v_i$ et $V' := \prod_i v_i'$. Enfin, notons $u_{\min} := \min(u_i)$ et $r := \min(u_{\min}, s)$.
Calculer la somme A du nombre de solutions des $s+1$ équations précédentes, en fonction de N, r, V, V'.

v. On suppose $N = 1$. Montrer que $p_1 - 1 = 2^{u_1} w_1$ et que $A = p_1 - 1$.

vi. On suppose $N > 1$. Montrer que $A \leq \frac{V}{V'} 2^{Nr} 2^{1-N}$ et calculer $\varphi(n)$ en fonction de U et V.
En déduire que si $\frac{\varphi(n)}{A} < 4$, alors $N = 2$, $a_1 = a_2 = 1$, $u_1 = u_2 = r$ et $V' = 1$, puis montrer que dans ce cas, $p_1 - 1$ et $p_2 - 1$ divisent $n - 1$.

vii. Conclure que dans tous les cas, si $n \neq 9$ est impair composé, alors au moins $\frac{3}{4}$ des entiers $1 \leq a < n$ premiers à n sont des témoins de Miller pour n.

viii. En déduire un test de primalité probabiliste, et estimer sa complexité et sa probabilité d'erreur.

Solution de l'exercice 3.

a) Soit a premier à n. Alors $a^{n-1} \equiv 1\ [n]$, donc $(a^t)^{2^s} \equiv 1\ [n]$. Notons $j := \min\{0 \leq k \leq s : (a^t)^{2^k} \equiv 1\ [n]\}$. Si $j = 0$, alors $a^t \equiv 1\ [n]$. Si $j \geq 1$, alors $(a^t)^{2^{j-1}}$ est une racine carrée de 1 modulo n, et ce n'est pas 1 modulo n. Donc nécessairement $(a^t)^{2^{j-1}} \equiv -1\ [n]$, d'où le résultat en posant $i := j - 1$.

b) i) On remarque que $561 - 1 = 2^4.35$, et on calcule $2^{35} \equiv 263\ [561]$, puis $2^{2.35} \equiv 166\ [561]$, puis $2^{2^2.35} \equiv 67\ [561]$, puis $2^{2^3.35} \equiv 1\ [561]$. Cela assure que 2 est un témoin de Miller pour 561 : cela démontre en effet que 561 n'est pas premier (c'est un nombre de Carmichael).

ii) On note g_0 un générateur de G. Écrivons une relation de Bezout : il existe $u, v \in \mathbb{Z}$ tels que $u.m + v.\#G = k$. Supposons qu'il existe $x \in G$ tel que $x^m = g$. Alors $g^{\frac{\#G}{k}} = x^{\frac{m\#G}{k}} = (x^{\frac{m}{k}})^{\#G} = 1$ par le théorème de Lagrange. Réciproquement, supposons que $g^{\frac{\#G}{k}} = 1$. On sait qu'il existe $r \in \mathbb{Z}$ tel que $g = g_0^r$. L'hypothèse $g^{\frac{\#G}{k}} = 1$ assure que k divise r (puisque g_0 engendre G), i.e. $r = k.r'$, avec $r' \in \mathbb{Z}$. On pose alors $x := g_0^{r'.u}$. Alors on a $x^m = g_0^{r'.u.m} = g_0^{k.r' - k.v.\#G} = g_0^{k.r'} = g_0^r = g$, donc l'équation a bien une solution.
Dans le cas où l'équation admet une solution $x_0 \in G$, on voit que $x \in G$ est solution si et seulement si $x.x_0^{-1}$ est d'ordre divisant m. Or il existe exactement k éléments de G dont l'ordre divise m (G est cyclique), donc l'équation admet exactement k solutions.

iii) i. C'est une conséquence directe de la question ii) (car 1 est solution).

ii. C'est une conséquence directe de la question ii) (car $g^2 = 1$).

iii. C'est une conséquence directe de la question ii) (car g n'est pas d'ordre impair).

iv. Le lemme chinois assure que toute équation de la forme $x^{2^{j-1}.t} = \pm 1$ dans G équivaut aux N équations $x_i^{2^{j-1}.t} = \pm 1$ dans $G_i := \mathbb{Z}/(p_i^{a_i}\mathbb{Z})^*$, avec $1 \leq i \leq N$. Or les G_i sont cycliques, donc on peut appliquer les questions i., ii. et iii. On obtient que le nombre $A_{i,j}$ de solutions de l'équation $x_i^{2^{j-1}.t} = -1$ dans G_i vaut $2^{j-1}.w_i$ si $1 \leq j \leq r$, que le nombre de solutions de $x_i^t = 1$ dans G_i vaut w_i, et que l'équation $x^{2^{j-1}.t} = -1$ n'a pas de solution dans G si $j > r$. Donc le nombre de solutions A recherché est

$$A = \prod_{i=1}^{N} w_i + \sum_{j=1}^{r} \prod_{i=1}^{N} A_{i,j} = \prod_{i=1}^{N} w_i + \sum_{j=1}^{r} \prod_{i=1}^{N} 2^{j-1}.w_i = \left(\prod_{i=1}^{N} w_i\right)\left(1 + \sum_{j=1}^{r} 2^{N.(j-1)}\right)$$

donc

$$A = \left(\prod_{i=1}^{N} w_i\right)\left(1 + \frac{2^{Nr}-1}{2^N-1}\right).$$

Or on a

$$\prod_{i=1}^{N} w_i = \frac{V}{V'},$$

donc finalement

$$A = \frac{V}{V'}\left(1 + \frac{2^{Nr}-1}{2^N-1}\right).$$

v. On a $N = 1$, donc $n = p_1^{a_1}$, donc $p_1 - 1$ divise $n - 1$, donc

$$p_1 - 1 = \text{pgcd}(p_1 - 1, n-1) = \text{pgcd}(p_1^{a_1-1}(p_1-1), n-1) = \text{pgcd}(2^{u_1}v_1, 2^s t) = 2^{u_1}.\text{pgcd}(v_1, t) = 2^{u_1}w_1.$$

Or la question précédente assure que $A = 2^{u_1}w_1$, donc finalement $A = p_1 - 1$.

vi. On a $A = \frac{V}{V'}\left(1 + \frac{2^{Nr}-1}{2^N-1}\right)$, donc on vérifie facilement que $A \leq \frac{V}{V'}2^{Nr}2^{1-N}$.
En outre,

$$\varphi(n) = \prod_{i=1}^{N} p_i^{a_i-1}(p_i - 1) = 2^U.V.$$

Supposons $\frac{\varphi(n)}{A} < 4$. Alors $V'.2^{N-1}.2^{U-Nr} < 4$. Or on a par définition $u_i \geq r$ pour tout i, donc $U \geq Nr$. De plus, pour tout i, puisque t divise $n-1$, alors p_i ne divise pas t, donc p_i divise V' dès que $a_i > 1$. Donc la condition $V'.2^{N-1}.2^{U-Nr} < 4$ assure que $N = 2$, $V' = 1$, $U = Nr$, $a_1 = a_2 = 1$. On en déduit aussi que $u_1 = u_2 = r$. Alors v_1 et v_2 divisent t, et $r \leq s$, donc $p_1 - 1$ et $p_2 - 1$ divisent $n - 1$.

vii. Si $N > 1$ et $\frac{\varphi(n)}{A} < 4$, alors $n = p_1.p_2$ et $p_i - 1$ divise $n - 1$. Ceci est impossible. Donc pour tout n tel que $N > 1$, on a $\frac{\varphi(n)}{A} \geq 4$. Dans le cas où $N = 1$, alors $n = p^a$ (avec $a \geq 2$) et $A = p - 1$, donc $\frac{\varphi(n)}{A} = p^{a-1} \geq 4$ dès que $n \neq 9$.

On a donc montré que pour tout entier impair composé n distinct de 9, $\frac{\varphi(n)}{A} \geq 4$, ce qui signifie exactement qu'au moins $\frac{3}{4}$ des entiers $1 \leq a < n$ premiers à n sont des témoins de Miller pour n.

viii. On choisit a premier à n entre 1 et n, au hasard (tirage uniforme), puis on fait le test de la question a). En cas de réponse négative, on sait que n n'est pas premier. Dans le cas contraire, on tire un nouvel a et on recommence. Après k tirages indépendants, la probabilité que l'entier n soit composé alors qu'il a passé les k tests est majorée par $\frac{1}{4^k}$. Pour k assez grand, on dira donc dans ce cas que n est probablement premier.

Exercice 4 : (Comparaison des tests de Solovay-Strassen et de Miller-Rabin)
Soit $n > 2$ impair. On note $n - 1 = 2^s t$.

a) Soit $1 \leq a < n$ tel que a ne soit pas un témoin de Miller pour n.
   i) On suppose $a^t \equiv 1\ [n]$. Montrer que $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]$.
   ii) On suppose qu'il existe $0 \leq i < s$ tel que $a^{2^i t} \equiv -1\ [n]$.
      i. Calculer $a^{\frac{n-1}{2}}$ modulo n.
      ii. Soit p premier divisant n. On note $p - 1 = 2^u v$. Montrer que $u \geq i + 1$, que $\left(\frac{a}{p}\right) = 1$ si $u > i + 1$ et que $\left(\frac{a}{p}\right) = -1$ si $u = i + 1$.
      iii. Vérifier que dans le premier cas, $p \equiv 1\ [2^{i+2}]$, et que dans le second, $p \equiv 1 + 2^{i+1}\ [2^{i+2}]$.
      iv. On note k le nombre de facteurs premiers p de n, comptés avec multiplicité, pour lesquels $u = i + 1$ (second cas). Montrer que $\left(\frac{a}{n}\right) = (-1)^k$ et $n \equiv 1 + k.2^{i+1}\ [2^{i+2}]$.
      v. En déduire que $n \equiv 1\ [2^{i+2}]$ si et seulement si k est pair.
      vi. En déduire que $i < s - 1$ si et seulement si k est pair.
      vii. En déduire que $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]$.

b) Expliquer en quel sens le test de Rabin-Miller est meilleur (au sens large) que le test de Solovay-Strassen.

Solution de l'exercice 4.

a) i) Puisque t est impair, on a

$$\left(\frac{a}{n}\right) = \left(\frac{a}{n}\right)^t = \left(\frac{a^t}{n}\right) = \left(\frac{1}{n}\right) = 1\,.$$

En outre, t divise $\frac{n-1}{2}$, donc $a^{\frac{n-1}{2}} \equiv 1\ [n]$. D'où finalement $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]$ $(\equiv 1\ [n])$.

ii) i. On a $\frac{n-1}{2} = 2^{s-1}t$, donc

$$a^{\frac{n-1}{2}} = (a^{2^i t})^{2^{s-1-i}} \equiv (-1)^{s-1-i}\ [n]$$

d'où finalement $a^{\frac{n-1}{2}} \equiv -1\ [n]$ si $i = s - 1$ et $a^{\frac{n-1}{2}} \equiv 1\ [n]$ si $i < s - 1$.

ii. On a $a^{2^i t} \equiv -1\ [n]$, donc $a^{2^i t} \equiv -1\ [p]$, donc a^t est d'ordre exactement 2^{i+1} modulo p. On a donc un élément d'ordre 2^{i+1} dans $(\mathbb{Z}/p\mathbb{Z})^*$, donc le théorème de Lagrange assure que 2^{i+1} divise $p - 1$, donc 2^{i+1} divise 2^u, donc $u \geq i + 1$. En outre on a

$$\left(\frac{a}{p}\right) = \left(\frac{a^t}{p}\right) \equiv a^{t.\frac{p-1}{2}} \equiv a^{2^{u-1}vt} \equiv (a^{2^i t})^{2^{u-1-i}v} \equiv (-1)^{2^{u-i-1}}\ [p]\,,$$

d'où le résultat.

iii. c'est évident.

iv. On écrit la décomposition de n en facteurs premiers de la façon suivante : $n = \prod_{p \in S_1} p^{r_p} \times \prod_{p \in S_2} p^{r_p}$ où S_1 (resp. S_2) désigne l'ensemble des premiers p divisant n tels que $u > i + 1$ (resp. $u = i + 1$). Alors la question ii. assure que

$$\left(\frac{a}{n}\right) = \prod_{p|n} \left(\frac{a}{p}\right)^{r_p} = \prod_{p \in S_2} (-1)^{r_p} = (-1)^{\sum_{p \in S_2} r_p} = (-1)^k\,.$$

En outre, l'écriture $n = \prod_{p \in S_1} p^{r_p} \times \prod_{p \in S_2} p^{r_p}$ et la question iii. assurent que

$$n \equiv \prod_{p \in S_2} (1 + 2^{i+1})^{r_p} \equiv (1 + 2^{i+1})^k\ [2^{i+2}]\,.$$

Or la formule du binôme montre que l'on a $(1 + 2^{i+1})^k \equiv 1 + k.2^{i+1}\ [2^{i+2}]$, d'où le résultat.

v. On a $n \equiv 1\ [2^{i+2}]$ si et seulement si 2^{i+2} divise $k.2^{i+1}$ si et seulement si k est pair.

vi. On a $n \equiv 1\ [2^{i+2}]$ si et seulement si 2^{i+2} divise $n-1 = 2^s t$ si et seulement si $i+2 \leq s$. La question précédente assure alors la conclusion.

vii. Les questions iv. et vi. assurent que $\left(\frac{a}{n}\right) = 1$ si et seulement si $i < s-1$. Or on a montré à la question i. que $a^{\frac{n-1}{2}} \equiv 1\ [n]$ si et seulement si $i < s-1$. D'où finalement dans tous les cas $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}\ [n]$.

b) On a montré à la question a) que si a n'était pas témoin de Miller pour n, alors a n'était pas témoin de Solovay-Strassen pour n. Par conséquent, tout témoin du test de Solovay-Strassen pour n est un témoin de Miller pour n. Cela signifie que, partant d'un entier composé n, le test de Rabin-Miller a davantage de chance (au moins autant en fait) que le test de Solovay-Strassen de trouver un témoin a qui démontre que n est composé. Ainsi, un entier probablement premier pour le test de Rabin-Miller est "plus probablement premier" que s'il était seulement probablement premier pour le test de Solovay-Strassen.

Exercice 5 : (Test de Lucas-Lehmer)
On considère un entier N de la forme $N = h2^n - 1$, avec $n > 1$, h impair et $0 < h < 2^{n+1} - 1$.
Soit $a \in \mathbb{N}$, $a \geq 3$. On définit les suites (V_n) et (S_n) de la façon suivante : $V_0 := 2$, $V_1 := a$ et $V_{i+1} := aV_i - V_{i-1}$; $S_1 := V_h$ et $S_{i+1} := S_i^2 - 2$. On suppose $\left(\frac{a-2}{N}\right) = 1$ et $\left(\frac{a+2}{N}\right) = -1$ et on pose $D := a^2 - 4$.

a) Montrer qu'il existe un diviseur premier p de N et un élément $x \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ tel que $x^2 = D$.

b) On pose $\alpha := \frac{(a+2+x)^2}{4(a+2)}$. Montrer que $\alpha = \frac{a+x}{2}$, que α est racine de $X^2 - aX + 1$ et que dans le sous-corps $\mathbb{F}_p$ de $\mathbb{F}_{p^2}$, on a les relations suivantes :

$$\begin{cases} V_i = \alpha^i + \alpha^{-i} \\ S_i = \alpha^{h2^{i-1}} + \alpha^{-h2^{i-1}} \end{cases}.$$

c) Montrer que $\alpha^{\frac{p+1}{2}} = \left(\frac{a+2}{p}\right)$.

d) On suppose que N divise S_{n-1}.

i) Montrer que 2^n divise l'ordre de α dans $\mathbb{F}_{p^2}^*$.

ii) En déduire qu'il existe des entiers k et m tels que $N = (2^n k - 1)(2^n m + 1)$.

iii) Montrer que si $N \neq p$, alors $k \geq 2$ ou $m \geq 2$, donc $h \geq 2^{n+1} - 1$.

iv) Conclure que N est premier.

e) On suppose N premier. Montrer que N divise S_{n-1}.

f) En déduire un test de primalité pour les entiers de la forme précédente.

g) Montrer que si $h \equiv (-1)^{n-1}\ [3]$, on peut prendre $a = 4$ dans les questions précédentes.

h) Pour tout $n > 1$, on note $M_n := 2^n - 1$ le n-ième nombre de Mersenne. Adapter le test de primalité pour les M_n et estimer sa complexité.

i) Montrer que $M_{11} = 2047$ n'est pas premier.

j) Montrer que $M_{17} = 131071$ est premier.

Solution de l'exercice 5.

a) Les hypothèses assurent que $\left(\frac{D}{N}\right) = -1$. Par conséquent, il existe un facteur premier p de N tel que $\left(\frac{D}{p}\right) = -1$. Alors D n'est pas un carré modulo p, donc la classe de D dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ n'est pas un carré. On considère alors un corps de rupture du polynôme (irréductible) $X^2 - D$ sur $\mathbb{F}_p$. Ce corps est une extension de degré 2 de $\mathbb{F}_p$, il est donc isomorphe au corps $\mathbb{F}_{p^2}$. Par construction, ce corps contient une racine du polynôme $X^2 - D$, donc il existe $x \in \mathbb{F}_{p^2}$ tel que $x^2 = D$ (il est clair que $x \notin \mathbb{F}_p$ car D n'est pas un carré dans $\mathbb{F}_p$).

b) Un calcul simple utilisant que $x^2 = a^2 - 4$ assure que $\alpha = \frac{a+x}{2}$. De même, un calcul simple assure que α est racine de $X^2 - aX + 1$. En outre, les relations coefficients racines assurent que la seconde racine de ce polynôme est $\alpha^{-1} = \frac{a-x}{2}$. La récurrence linéaire double $V_{i+1} = aV_i - V_{i-1}$ assure que V_i dans $\mathbb{F}_{p^2}$ est une combinaison linéaire des suites (α^i) et (α^{-i}) (puisque le polynôme caractéristique de cette suite récurrente double n'est autre que $X^2 - aX + 1$ qui admet α et α^{-1} comme racines distinctes). On écrit donc qu'il existe $\lambda, \mu \in \mathbb{F}_{p^2}$ tels que pour tout i, $V_i = \lambda\alpha^i + \mu\alpha^{-i}$. Les conditions initiales $V_0 = 2$ et $V_1 = a$ assurent alors que $\lambda = \mu = 1$, donc pour tout i, on a $V_i = \alpha^i + \alpha^{-i}$. La dernière formule se démontre par récurrence : le cas $i = 1$ est une conséquence de la formule pour V_i. En effet, on a $S_1 = V_h = \alpha^h + \alpha^{-h}$. Pour l'hérédité, on remarque que si $S_i = \alpha^{h.2^{i-1}} + \alpha^{-h.2^{i-1}}$, alors la relation de récurrence $S_{i+1} = S_i^2 - 2$ assure que $S_{i+1} = \left(\alpha^{h.2^{i-1}} + \alpha^{-h.2^{i-1}}\right)^2 - 2 = (\alpha^{h.2^{i-1}})^2 + (\alpha^{-h.2^{i-1}})^2 + 2 - 2 = \alpha^{h.2^i} + \alpha^{-h.2^i}$, d'où la formule recherchée par récurrence.

c) On utilise la formule $\alpha = \frac{(a+2+x)^2}{4(a+2)}$. On a donc dans le corps $\mathbb{F}_{p^2}$, en utilisant que ce corps est de caractéristique p :

$$\alpha^{\frac{p+1}{2}} = \frac{(a+2+x)^{p+1}}{2^{p+1}(a+2)^{\frac{p+1}{2}}} = \frac{(a+2+x^p)(a+2+x)}{4(a+2)^{\frac{p+1}{2}}}.$$

Or $x \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ et $x^2 \in \mathbb{F}_p$, donc on vérifie que $x^p = -x$, d'où finalement

$$\alpha^{\frac{p+1}{2}} = \frac{(a+2-x)(a+2+x)}{4(a+2)^{\frac{p+1}{2}}} = \frac{(a+2)^2 - (a^2-4)}{4(a+2)^{\frac{p+1}{2}}} = \frac{(a+2)-(a-2)}{4(a+2)^{\frac{p-1}{2}}} = \frac{1}{(a+2)^{\frac{p-1}{2}}}.$$

Or on a $(a+2)^{\frac{p-1}{2}} \equiv \left(\frac{a+2}{p}\right)\ [p]$, donc finalement on a $\alpha^{\frac{p+1}{2}} = \left(\frac{a+2}{p}\right)$ dans $\mathbb{F}_p$.

d) i) L'hypothèse $S_{n-1} \equiv 0\ [N]$ implique que $S_{n-1} = 0$ dans $\mathbb{F}_p$, donc $\alpha^{h.2^{n-1}} = -1$ dans $\mathbb{F}_p$. Cela assure que α^h est d'ordre 2^n exactement. Cela assure immédiatement que l'ordre de α est divisible par 2^n.

ii) La question c) assure que $\alpha^{p+1} = 1$, donc $p+1$ est divisible par l'ordre de α, donc par 2^n. Donc il existe un entier $k \geq 1$ tel que $p = 2^n k - 1$. En notant $q := \frac{N}{p} \in \mathbb{N}$, on a alors $2^n h - 1 = N = (2^n k - 1)q$. On voit donc que q est congru à 1 modulo 2^n, donc q s'écrit $2^n m + 1$, avec $m \geq 0$ entier.

iii) Si $N \neq p$, alors $m \geq 1$. On a donc $2^n h - 1 = 2^{2n} km + 2^n(k-m) - 1$. Si $k = m = 1$, alors cette relation modulo 2^{2n} implique que h est pair, ce qui est exclu. Donc $k \geq 2$ ou $m \geq 2$. Alors la relation précédente implique que $h = 2^n km + k - m = m(2^n k - 1) + k$. Le fait que k ou m soit supérieur ou égal à 2 assure alors facilement que $h > 2^{n+1} - 1$.

iv) La conclusion de la question iii) est contradictoire avec l'hypothèse. Donc $N = p$, i.e. N est premier.

e) Si N est premier, alors la question c) assure que $\alpha^{2^{n-1}} = \left(\frac{a+2}{N}\right) = -1$, ce qui implique via la question b) que $S_{n-1} = 0$ dans $\mathbb{F}_N$. D'où le résultat.

f) On a montré finalement que N était premier si et seulement si N divise S_{n-1}. À a fixé, cela fournit un test de primalité pour N de complexité $\mathcal{O}(\log(n)\log(N)^2) = \mathcal{O}(n^2\log(n))$.

g) On suppose $h \equiv (-1)^{n-1}\ [3]$. On doit montrer que $\left(\frac{2}{N}\right) = 1$ et $\left(\frac{6}{N}\right) = -1$. La loi de réciprocité quadratique assure que $\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$. Or $N^2 - 1$ est divisible par 2^{n+1}, d'où le résultat dès que $n \geq 3$. De même, on a $\left(\frac{6}{N}\right) = \left(\frac{2}{N}\right)\left(\frac{3}{N}\right) = \left(\frac{3}{N}\right)$ pour $n \geq 3$. Par la loi de réciprocité quadratique, on a $\left(\frac{3}{N}\right) = (-1)^{\frac{N-1}{2}}\left(\frac{N}{3}\right)$. Or $\frac{N-1}{2} = h.2^{n-1} - 1$ est impair, donc il suffit de montrer que $\left(\frac{N}{3}\right) = 1$. Or $N = h.2^n - 1 \equiv (-1)^{n-1}.(-1)^n - 1 \equiv 1\ [3]$, donc $\left(\frac{N}{3}\right) = \left(\frac{1}{3}\right) = 1$. On peut donc bien prendre $a = 4$ dans le cas particulier où $h = (-1)^{n-1}$.

h) Si $n \geq 3$ est pair (plus généralement si n n'est pas premier), alors il est clair que M_n n'est pas premier ($2^{dr} - 1$ est divisible par $2^d - 1$). Donc on peut supposer n impair (et même premier impair). Dans ce cas, on a bien $h = 1 = (-1)^{n-1}$, donc on peut appliquer la question g) pour prendre $a = 4$, et ensuite appliquer le test de la question f) avec $a = 4$. Il suffit donc de tester si N divise S_{n-1}, dans le cas $a = 4$. Sa complexité est $\mathcal{O}(n^2 \log(n)) = \mathcal{O}(\log(M_n)^2 \log(\log(M_n)))$.

i) On vérifie que l'on a $S_{10} \equiv 282$ [2047], ce qui assure que $M_{11} = 2047$ n'est pas premier.

j) On calcule S_{16} modulo M_{17}, et on trouve que $S_{16} \equiv 0$ [M_{17}], donc $M_{17} = 131071$ est un nombre premier.