Notations, rappels et présentation du problème.

L'ensemble des entiers naturels sera noté $\mathbf{N}$, celui des entiers relatifs $\mathbf{Z}$.On notera $(\mathbf{Z}/n\mathbf{Z})^*$ l'ensemble des éléments de $\mathbf{Z}/n\mathbf{Z}$ inversibles pour la multiplication.

Etant donnés deux entiers relatifs a et b , le plus grand diviseur commun de a et b sera noté PGCD(a, b) ou $a \wedge b$. On rappelle que $a \wedge 0 = a$.
a est dit premier avec b si $a \wedge b = 1$.
$a \equiv b \, mod \, n$ signifie que a est congru à b modulo n, c'est-à-dire que n divise $(b - a)$.

Un groupe (G,×) est dit cyclique s'il existe un élément a de G et un entier naturel p tel que G = $\left\{1, a, a^2, a^3, ..., a^p\right\}$, où $a^k = a \times a \times ... \times a$ (k termes) ; a est alors un générateur de (G,×).

Pour un entier naturel n supérieur ou égal à 2, on notera respectivement :
S_n l'ensemble des entiers strictement positifs, inférieurs ou égaux à n, et premiers avec n.
D_n l'ensemble des diviseurs de n, entiers positifs (en particulier, 1 appartient à D_n).

La notation $\sum_{d \in D_n}$ désignera une somme étendue à tous les éléments d de D_n.

Enfin on notera $\phi(n)$ le cardinal de S_n.

La première partie du problème a pour but d'établir une identité due à Euler concernant la fonction ϕ, à l'aide d'un raisonnement probabiliste.

Dans la deuxième partie, on étudie le groupe des éléments inversibles pour la multiplication dans $\mathbf{Z}/n\mathbf{Z}$, et on montre que, si n n'a qu'un seul diviseur premier, alors ce groupe est cyclique.

La troisième partie introduit la notion de nombres pseudo-premiers forts et se propose d'en donner une caractérisation algorithmique sur une calculatrice programmable.

Enfin, la quatrième partie a pour objet l'étude de nombres appelés nombres de Carmichaël, présentant des similarités avec les nombres premiers, et se termine par la présentation d'un test probabiliste pour la détection de nombres premiers.

Partie I

1. On considère dans cette question un univers probabilisé (Ω, B, P). L'événement contraire d'un événement E sera noté $\overline{E}$
   (a) Soient A_1 et A_2 deux événements indépendants de cet univers : montrer que $\overline{A}_1$ et A_2 sont indépendants.
   (b) Généralisation : soit k un entier naturel non nul et $A_1, A_2, ...A_k$ k événements mutuellement indépendants de Ω.
      (I) Montrer que $\overline{A_1}, A_2, ...A_k$ sont indépendants.
      (II) Montrer par récurrence que $\overline{A_1}, \overline{A_2}, ...\overline{A_k}$ sont indépendants.

   Dans toute la suite de cette partie, n désigne un entier naturel supérieur ou égal à 2 et X une variable aléatoire sur Ω, prenant ses valeurs dans l'ensemble $\{1, .., n\}$ de manière équiprobable, c'est-à-dire telle que pour tout $i = 1, .., n$ on a $P(X = i) = \dfrac{1}{n}$.

2. On considère l'événement A_1 : "X est multiple de 2" et l'événement A_2 : "X est multiple de 5"
   (a) On suppose que $n = 100$.
   Calculer les probabilités des événements A_1 et A_2. A_1 et A_2 sont-ils indépendants ?
   (b) On suppose maintenant que $n = 101$. Reprendre les questions du (a) dans ce cas.

3. On suppose que la décomposition en facteurs premiers de n s'écrit $n=\prod_{i=1}^{k} p_i^{\alpha_i}$, où les α_i sont des entiers supérieurs ou égaux à 1.
   Enfin, pour i entier naturel, $1 \leq i \leq k$, A_i désigne l'événement "X est divisible par p_i".
   (a) Soit A l'événement : "X est premier avec n" ; exprimer P(A) à l'aide de n et de $\phi(n)$.
   (b) Montrer que $P(A_i) = \dfrac{1}{p_i}$ pour tout entier i, $1 \leq i \leq k$.
   (c) Montrer que les $(A_i)_{1 \leq i \leq k}$ sont mutuellement indépendants.
   (d) Exprimer A à l'aide des $\overline{A_i}$.
   (e) En déduire que $\phi(n) = n \prod_{i=1}^{k} (1 - \dfrac{1}{p_i})$ (E).

4. On se propose de retrouver l'égalité précédente (E) par une autre méthode : soient p et q deux entiers naturels premiers entre eux ;
   On considère l'application h: $\begin{cases} S_{pq} \to \{0, ..., p-1\} \times \{0, ..., q-1\} \\ r \to (a, b) \end{cases}$ où a (resp b) est le reste de la division de r par p (resp par q).
   (a) Montrer que h(S_{pq}) est inclus dans $S_p \times S_q$.
   (b) Montrer que h est injective.
   (c) Justifier l'existence de deux entiers α et β de $\mathbf{Z}$ tels que : $\alpha p + \beta q = 1$.
   Soit (a, b) un couple de $S_p \times S_q$. On note $x = \alpha pb + \beta qa$; montrer que $x \equiv a \bmod p$ et que $x \equiv b \bmod q$.
   En déduire que l'image de h est $S_p \times S_q$, puis que $\phi(pq) = \phi(p)\phi(q)$.
   (d) A l'aide d'une récurrence sur le nombre de diviseurs premiers de n, retrouver alors l'égalité (E).

5. Identité d'Euler :
   (a) Soit d un diviseur de n et a un entier naturel non nul ; montrer que PGCD$(a, n) = d$ si, et seulement si, il existe un entier k premier avec $\frac{n}{d}$ tel que $a = kd$. En déduire le nombre des entiers a tels que $1 \leq a \leq n$ et PGCD$(a, n) = d$.
   (b) Pour tout entier d diviseur de n, on note C_d l'événement "PGCD(X,n)=d".

   Exprimer P(C_d) à l'aide de n, d et de la fonction ϕ
   (c) En déduire que $\sum_{d \in D_n} \frac{1}{n}\phi(\frac{n}{d}) = 1$ (rappel : D_n note l'ensemble des diviseurs de n dans **N**).
   (d) Montrer que l'application u qui, à tout diviseur d de n associe u(d)=$\frac{n}{d}$ est une bijection de D_n dans lui-même. Montrer que $\sum_{d \in D_n} \phi(d) = n$ (identité d'Euler).

Partie II

n étant toujours un entier supérieur ou égal à 2, l'objet de cette partie est l'étude du groupe noté $\left((\mathbf{Z}/n\mathbf{Z})^*, \times\right)$ des éléments de $\mathbf{Z}/n\mathbf{Z}$ inversibles pour la multiplication.

On rappelle que cet ensemble est composé des classes modulo n des nombres premiers avec n. On pourra donc remarquer que $\phi(n) = card\left((\mathbf{Z}/n\mathbf{Z})^*\right)$.
La classe d'un entier a sera notée $\dot{a}$.

A) Des résultats généraux sur les groupes et les anneaux.

1. Soient a et b deux éléments d'un anneau commutatif (A,+,×) et n un entier naturel non nul. Montrer que $b^n - a^n$ est divisible par $b - a$.
   Donner le quotient de $b^n - a^n$ par $b - a$ sous forme de somme.

2. Montrer que $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ est un corps si, et seulement si, n est premier.

3. Factorisation de polynômes.
   (a) Soit P un polynôme de degré k supérieur ou égal à 1, à coefficients dans $\mathbf{Z}/n\mathbf{Z}$, où n est un entier premier.

   Montrer que P admet au plus k racines (on pourra raisonner par récurrence sur k).
   (b) Déterminer, dans $\mathbf{Z}/6\mathbf{Z}$, les racines du polynôme P(X)=X^2-X. Que peut-on en conclure ?
   (c) Trouver, dans $\mathbf{Z}/6\mathbf{Z}[X]$, deux factorisations distinctes de X^2-X sous la forme (X-$\dot{a}$)(X-$\dot{b}$).

4. On rappelle que si x est élément d'un groupe fini G, l'ordre de x est le plus petit entier naturel k non nul tel que $x^k = 1$, où 1 désigne l'élément neutre de G.
   (a) Soit x un élément de G, groupe fini de cardinal n ; montrer que, si k est l'ordre de x, alors l'ensemble $\{1, x, ..., x^{k-1}\}$ est un sous-groupe de G.

   En déduire que l'ordre de x divise le cardinal de G, et que $x^n = 1$.
   (b) Si p est un entier naturel premier et x un entier naturel non divisible par p, montrer que $x^{p-1} - 1$ est divisible par p.

B) Etude du groupe $\left((\mathbf{Z}/n\mathbf{Z})^*, \times\right)$ quand n est premier.

On suppose dans cette sous-partie que n est un entier premier supérieur ou égal à 3. Si d est un entier naturel non nul et strictement inférieur à n, on note $\zeta(d)$ le nombre des éléments de $\left((\mathbf{Z}/n\mathbf{Z})^*, \times\right)$ d'ordre d.

1. Montrer que $\sum_{d \in D_{n-1}} \zeta(d) = n - 1$.

2. Soit d un diviseur de $n-1$ et soit $\dot{a}$ un élément de $\left((\mathbf{Z}/n\mathbf{Z})^*, \times\right)$ d'ordre d, s'il existe.
   $\dot{a}$ vérifie ainsi $\dot{a}^d = \dot{1}$.
   (a) Montrer que l'ensemble des racines du polynôme $X^d - \dot{1}$ est, dans $(\mathbf{Z}/n\mathbf{Z})^*$, $\left\{\dot{1}, \dot{a}, \dot{a}^2, \dot{a}^3, ..., \dot{a}^{d-1}\right\}$.
   (b) On suppose que k est un entier naturel inférieur ou égal à d, non premier avec d. Montrer que $\dot{a}^k$ a un ordre strictement inférieur à d.
   (c) En déduire que $\zeta(d) \leq \phi(d)$.

   Déduire des questions précédentes et de la première partie que $\zeta(d) = \phi(d)$ pour tout diviseur d de $n-1$.

   Montrer en particulier qu'il existe au moins un élément $\dot{b}$ d'ordre $n-1$ dans $\left((\mathbf{Z}/n\mathbf{Z})^*, \times\right)$ et que $(\mathbf{Z}/n\mathbf{Z})^* = \left\{\dot{1}, \dot{b}, \dot{b}^2, ...\dot{b}^{n-2}\right\}$.

C) Cas n=p$^\alpha$.

On suppose maintenant que n s'écrit sous la forme $n = p^\alpha$, où p est un entier premier, et α un entier naturel supérieur ou égal à 2.

D'après la partie II B), il existe donc un entier b, dont la classe $\dot{b}$ est d'ordre $p-1$ dans $\left((\mathbf{Z}/p\mathbf{Z})^*, \times\right)$.

1. Montrer que l'un au moins des deux entiers b^{p-1} ou $(b+p)^{p-1}$ n'est pas congru à 1 modulo p^2 ; on notera c l'un des nombres b ou $b+p$ de façon à ce que c^{p-1} ne soit pas congru à 1 modulo p^2.

2. Montrer par récurrence que, pour tout entier naturel r, il existe un entier k_r premier avec p tel que $c^{p^r(p-1)} = 1 + k_r \times p^{r+1}$. En déduire que $\dot{c}$ appartient à $(\mathbf{Z}/n\mathbf{Z})^*$.

3. Soit r l'ordre de $\dot{c}$ dans $\left((\mathbf{Z}/n\mathbf{Z})^*, \times\right)$.
   (a) Expliquer pourquoi r divise $p^{\alpha-1}(p-1)$ et pourquoi $(p-1)$ divise r.
   (b) En déduire qu'il existe un entier naturel β inférieur ou égal à $\alpha - 1$ tel que $r = p^\beta(p-1)$.
   (c) Montrer finalement que $\beta = \alpha - 1$ et que $\dot{c}$ est un générateur de $\left((\mathbf{Z}/n\mathbf{Z})^*, \times\right)$.

4. Application : Déterminer un générateur de $\left((\mathbf{Z}/7\mathbf{Z})^*, \times\right)$ puis un générateur de $\left((\mathbf{Z}/49\mathbf{Z})^*, \times\right)$.

Partie III

Nombres pseudo-premiers forts

Dans toute cette partie, p désigne un entier impair supérieur ou égal à 3, et on notera $(p-1) = q \times 2^s$, où q est un entier naturel impair et s un entier naturel supérieur ou égal à 1.

1. Dans cette question, on suppose p premier.
   (a) Soit a un entier premier avec p. Montrer que $a^{\frac{p-1}{2}}$ est congru à 1 ou à $p-1$ modulo p.
   (b) On dit qu'un entier naturel a vérifie la propriété $H_a(p)$ si :
   $(a^q \equiv 1 \bmod p)$ *ou* ($\exists$ r entier, $0 \leq r < s$ tel que $a^{q \times 2^r} \equiv p-1 \bmod p$) $H_a(p)$

   Montrer que tout entier naturel a premier avec p vérifie $H_a(p)$.

2. On dit qu'un nombre p impair, non nécessairement premier, est pseudo-premier fort en base a si la propiété $H_a(p)$ est vérifiée ; on écrira en abrégé que p est a-ppf.

   Par exemple, 25 est 7-ppf car 24=3*2^3 et $7^{3\times 2} = 117649 \equiv 24 \equiv -1 \bmod 25$.

   Montrer que si a est un entier tel que le pgcd de a et p est strictement plus grand que 1, alors p ne peut pas être a-ppf.

3. Construction d'un algorithme :
   (a) Un entier p impair et un entier a étant donnés, écrire un algorithme permettant de tester si p est a-ppf.

   N.B. : On ne cherchera pas à écrire, pour le calcul de a^q modulo p un algorithme rapide de puissance, mais on pourra se contenter d'une boucle calculant a^2 modulo p, a^3 modulo p, ..., a^q modulo p.

   Vous retranscrirez cet algorithme sur votre copie en langage algorithmique (français) ou dans le langage de votre machine, en spécifiant le modèle que vous employez.

   Implanter cet algorithme sur votre machine ; on peut le tester en contrôlant que tout nombre p premier est a-ppf pour tout a premier avec p.

   (b) Reportez le tableau suivant sur votre copie et complétez les cases vides par "oui" ou "non" à l'aide du programme précédent.

p	49	91	111	121	135	1225
a	30	74	28	94	43	999
p est a-ppf						

   (c) On peut vérifier (la vérification n'est pas demandée) que l'ensemble des entiers a, compris au sens large entre 1 et 560 tels que 561 soit a-ppf. est $\{1, 50, 101, 103, 256, 305, 458, 460, 511, 560\}$.

   Montrer que l'ensemble des classes modulo 561 de ces entiers constitue un sous-groupe cyclique de $\left((\mathbf{Z}/561\mathbf{Z})^*, \times\right)$.

Partie IV

A) Nombres de Carmichaël

L'objet de cette partie est la caractérisation de certains nombres, appelés nombres de Carmichaël.
On rappelle que pour tout entier naturel premier p, et tout a entier premier avec p, $a^{p-1} \equiv 1 \bmod p$.

La réciproque n'est pas vraie ; un nombre n est appelé nombre de Carmichaël si :

a) n n'est pas premier
b) pour tout nombre a premier avec n, a^{n-1} est congru à 1 modulo n.

1. Montrer que si $n = p_1 \times p_2 \times .... \times p_k$ où $p_1, p_2, ..., p_k$ sont des nombres premiers deux à deux distincts tels que $(p_i - 1)$ divise $(n-1)$ pour tout i de $\{1, 2, ..., k\}$, alors n est un nombre de Carmichaël.

   Montrer en particulier que 561, 10585 sont des nombres de Carmichaël.

2. Dans toute cette question, on suppose que n est un nombre de Carmichaël et l'on désire établir la réciproque du résultat obtenu en question 1.

   (a) On suppose tout d'abord que n est une puissance de 2, $n = 2^\alpha$, où α est un entier ≥ 2.

   Quel est le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$? En déduire que pour tout entier a impair $a^{(2^\alpha - 1)}$ ne peut être congru à 1 modulo n sauf si a est congru à 1 modulo n ; que peut-on conclure ?

   (b) On suppose désormais que n admet au moins un facteur premier impair p_1 et l'on note $p_1, p_2, ..., p_k$ les facteurs premiers de n ; la décomposition de n est alors $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

   (I) Soit ω un entier dont la classe modulo $p_1^{\alpha_1}$ est un générateur de $\left((\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^*, \times\right)$; ω existe d'après la partie II. A l'aide de la bijection définie dans la question I 4, montrer qu'on peut trouver un entier t tel que :

   $t \equiv \omega \bmod p_1^{\alpha_1}$ et, pour tout i (s'il en existe) tel que $2 \leq i \leq k$, $t \equiv 1 \bmod p_i^{\alpha_i}$.

   Montrer qu'alors $t^{n-1} \equiv 1 \bmod n$.

   (II) En déduire que $p_1^{\alpha_1 - 1}(p_1 - 1)$ divise $(n-1)$, puis que $\alpha_1 = 1$, et enfin que $(p_1 - 1)$ divise $(n-1)$.

   (III) Montrer que n est nécessairement impair et que n peut s'écrire sous la forme $n = p_1 \times p_2 \times .... \times p_k$ où $p_1, p_2, ..., p_k$ sont des nombres premiers deux à deux distincts tels que ($p_i - 1$) divise $(n-1)$ pour tout i de $\{1, 2, ..., k\}$ .Conclure.

3. Montrer qu'un nombre de Carmichaël admet au moins trois facteurs premiers.

4. Résoudre l'équation $85p - 16k = 1$, où (k, p) appartient à $\mathbf{Z}^2$.

   Déterminer le plus petit nombre de Carmichaël divisible par 5 et 17.

B) Le test de Miller-Rabin

1. Soit n un nombre non premier et qui ne soit pas non plus un nombre de Carmichaël.

   Montrer qu'il existe au moins un entier a inférieur à n et premier avec n tel que n ne soit pas a-ppf.

2. En fait, on peut démontrer et l'on admettra que, pour tout nombre n non premier, l'ensemble des classes des entiers naturels a strictement inférieurs à n tels que n soit a-ppf est inclus dans un sous-groupe strict de $\left((\mathbf{Z}/n\mathbf{Z})^*, \times\right)$.
   Le test de Miller-Rabin est alors le suivant : étant donnés un nombre impair n et un entier k, on effectue k épreuves indépendantes ; l'épreuve n°i $(i = 1, ..., k)$ consistant à choisir un entier a_i de manière équiprobable parmi $\{1, 2, 3, ..., n-1\}$ et à tester la propriété "n est a_i-ppf".
   - Si, pour l'un des a_i, n n'est pas a_i-ppf, n est composé.
   - Si n est pseudo-premier fort pour tous les a_i, alors n est déclaré premier.

   On suppose que n est composé (c'est-à-dire non premier) ; par quelle valeur (en fonction de k), peut-on majorer la probabilité de déclarer n premier ?