Capes 2003 - Deuxième épreuve

Cette correction a été rédigée par Frédéric Bayart. Si vous avez des remarques à faire, ou pour signaler des erreurs, n'hésitez pas à écrire à : mathweb@free.fr

Mots-clés : Probabilités, événements indépendants, identité d'Euler, arithmétique, anneau, Z/nZ

Commentaires : Le premier problème commence par des probabilités, ce qui est assez inhabituel. Les questions ne sont pas très difficiles, mais il faut avoir les idées claires sur le vocabulaire, et notamment sur celui concernant les événements indépendants. Du reste, de nombreux résultats que ce problème propose de démontrer sont ou du cours, ou des choses très classiques. C'est d'autre part un excellent problème pour vérifier que l'on est au point en arithmétique, notamment au niveau des groupes Z/nZ, des classes de congruence, et des théorèmes classiques (Gauss, Fermat,...).

Partie 1

1.a. Rappelons que deux événements sont indépendants si, et seulement si, $P(A_1 \cap A_2) = P(A_1)P(A_2)$. Supposons donc que A_1 et A_2 sont indépendants. On a :

$$\begin{aligned} P(A_2) &= P(A_1 \cap A_2) + P(\overline{A_1} \cap A_2) \\ &= P(A_1)P(A_2) + P(\overline{A_1} \cap A_2) \end{aligned}$$

On en déduit :

$$\begin{aligned} P(\overline{A_1} \cap A_2) &= [1 - P(A_1)]P(A_2) \\ &= P(\overline{A_1})P(A_2). \end{aligned}$$

1.b.i. Rappelons que k événements $A_1, \ldots, A_k$ sont mutuellement indépendants si, et seulement si, pour tout $J \subset \{1, \ldots, k\}$,

$$P\left(\bigcap_{j \in J} A_j\right) = \prod_{j \in J} P(A_j).$$

Soit donc $J \subset \{1, \ldots, k\}$. Si $1 \notin J$, l'égalité précédente est clairement vérifiée. Sinon, on écrit $J = \{1\} \cup J'$, et on note $B = \bigcap_{j \in J'} A_j$. D'après 1.a., puisque A_1 et B sont indépendants,

$$P(\overline{A_1} \cap B) = P(\overline{A_1})P(B).$$

On utilise l'indépendance mutuelle de $A_2, \ldots, A_k$ pour conclure que

$$P(\overline{A_1} \cap B) = P(\overline{A_1}) \prod_{j \in J'} P(A_j).$$

$\overline{A_1}, A_2, \ldots, A_k$ sont (mutuellement) indépendants.

1.b.ii. Montrons par récurrence sur j, $1 \leq j \leq k$, que $\overline{A_1},\ldots,\overline{A_j},A_{j+1},\ldots,A_k$ sont indépendantes. C'est fait pour $j=1$, et si c'est vrai jusqu'au rang j, les événements $A_{j+1},\overline{A_1},\ldots,\overline{A_j},A_{j+2},\ldots,A_k$ sont indépendants. La question précédente garantit que $\overline{A_{j+1}},\overline{A_1},\ldots,\overline{A_j},A_{j+2},\ldots,A_k$ sont indépendants, ce qui, quitte à réordonner les événements, est le résultat attendu.

2.a. On a :

$$P(A_1) = \frac{\text{nombre de cas favorables}}{\text{nombre de cas possibles}}.$$

Il y a 50 nombres qui sont multiples de 2 dans $\{1,\ldots,100\}$, d'où :

$$P(A_1) = \frac{50}{100} = \frac{1}{2}.$$

De même, $P(A_2) = \frac{20}{100} = \frac{1}{5}$. A_1 et A_2 sont indépendants :

$$A_1 \cap A_2 = \{X \text{ est multiple de } 10\}.$$

$$P(A_1 \cap A_2) = \frac{10}{100} = \frac{1}{10} = P(A_1)P(A_2).$$

2.b. On a désormais $P(A_1) = \frac{50}{101}$, $P(A_2) = \frac{20}{101}$, et $P(A_1 \cap A_2) = \frac{10}{101}$. Or,

$$P(A_1)P(A_2) = \frac{1000}{(101)^2} \neq \frac{10}{101}.$$

A_1 et A_2 ne sont pas indépendants.

3.a. Il est clair que :

$$P(A) = \frac{\phi(n)}{n}.$$

3.b. Les nombres divisibles par p_i entre 1 et n s'écrivent $p_i \times r$, où $1 \leq r \leq \frac{n}{p_i}$. Il y a donc $\frac{n}{p_i}$ tels nombres, et

$$P(A_i) = \frac{n/p_i}{n} = \frac{1}{p_i}.$$

3.c. Soit $J \subset \{1,\ldots,k\}$; on écrit $J = \{i_1,\ldots,i_u\}$. $A_{i_1} \cap \cdots \cap A_{i_u}$ est l'événement $\{X$ est divisible par $p_{i_1}\ldots p_{i_u}\}$. Le même raisonnement qu'en b. prouve que :

$$\begin{aligned} P(A_{i_1} \cap \cdots \cap A_{i_u}) &= \frac{n}{p_{i_1}\ldots p_{i_u}} \times \frac{1}{n} = \frac{1}{p_{i_1}\ldots p_{i_u}} \\ &= P(A_{i_1})\ldots P(A_{i_u}). \end{aligned}$$

Les événements (A_i) sont mutuellement indépendants.

3.d. Il est clair que :

$$\begin{aligned} X \text{ premier avec } n &\iff X \text{ premier avec } p_1,\ldots,p_k \\ &\iff p_1,\ldots,p_k \text{ ne divise pas } n. \end{aligned}$$

On a donc : $A = \overline{A_1} \cap \cdots \cap \overline{A_k}$.

3.e. Grâce à la question 1., $\overline{A_1},\ldots,\overline{A_k}$ sont indépendants, et :

$$\begin{aligned} P(A) &= P(\overline{A_1})\ldots P(\overline{A_k}) \\ &= \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right). \end{aligned}$$

Puisqu'on a déjà prouvé que $P(A) = \frac{n}{\phi(n)}$, on en déduit le résultat.

4.a. D'après les propriétés de la division euclidienne et du pgcd (algorithme d'Euclide du calcul du pgcd), on a :

$$r \wedge p = p \wedge a.$$

Puisque $r \wedge pq = 1$, on a $r \wedge p = 1$ et donc a est premier avec p, d'où $a \in S_p$. De même, on prouve que $b \in S_q$.

4.b. Si on avait $h(r) = h(r') = (a,b)$, on aurait :

$$\left\{ \begin{array}{rclrcl} r & = & k_1 p + a & r' & = & k'_1 p + a \\ r & = & k_2 q + b & r' & = & k'_2 q + b \end{array} \right.$$

On en déduit que $p|r - r'$ et $q|r - r'$. Comme p et q sont premiers entre eux, on obtient $pq|r - r'$. Puisque $1 \leq r,r' \leq pq$, on a forcément $r = r'$.

4.c. L'existence de α et β est une conséquence de l'identité de Bézout. On a donc :

$$x = \alpha pb + \beta qa = p(\alpha b - \alpha a) + a,$$

ce qui donne $x \equiv a \mod p$. De même, $x \equiv b \mod q$. Ceci entraîne en particulier que $x \wedge p = 1$ et $x \wedge q = 1$. Puisque p et q sont premiers entre eux, on a en particulier $x \wedge pq = 1$. Soit alors $x_0 \in S_{pq}$ tel que $x \equiv x_0 \mod (pq)$. On a en particulier

$$x_0 \equiv a \mod p,\ x_0 \equiv b \mod q,$$

et donc $h(x_0) = (a,b)$. Ainsi, $h(S_{pq}) = S_p \times S_q$, et h réalise une bijection de S_{pq} sur $S_p \times S_q$. D'où l'identité :

$$\phi(pq) = \phi(p)\phi(q).$$

4.d. Une récurrence immédiate prouve que :

$$\phi\left(p_1^{\alpha_1} \dots p_k^{\alpha_k}\right) = \phi\left(p_1^{\alpha_1}\right) \dots \phi\left(p_k^{\alpha_k}\right).$$

Reste à calculer $\phi\left(p_i^{\alpha_i}\right)$: si $x \in S_{p_i^{\alpha_i}}$, on a $1 \leq x \leq p_i^{\alpha_i}$, et $x \wedge p_i = 1$. Or, les multiples de p_i dans $\{1, \dots, p_i^{\alpha_i}\}$ s'écrivent $p_i \times r$, où $1 \leq r \leq p_i^{\alpha_i - 1}$. On a donc :

$$\phi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right).$$

5.a. Si $PGCD(a,n) = d$, on écrit $a = k_1 d$, $n = k_2 d$, où $k_1 \wedge k_2 = 1$. C'est exactement le résultat demandé, et la réciproque est aussi immédiate. Le nombre recherché vaut donc $\phi(n/d)$ (car $a \leq n \implies k \leq n/d$).

5.b. On a, en fonction de la question précédente :

$$P(C_d) = \frac{\phi(n/d)}{n}.$$

5.c. Les événements $(C_d)_{d|n}$ forment un système complet d'événements. Autrement dit, ils sont deux à deux disjoints (le pgcd est unique), et leur réunion forme l'univers tout entier. On a donc :

$$\sum_{d|n} P(C_d) = 1,$$

ou encore

$$\sum_{d \in D_n} \frac{1}{n} \phi\left(\frac{n}{d}\right) = 1.$$

5.d. Le fait que u est une bijection est (presque) évident. Le changement de variables $d \mapsto u(d)$ dans le résultat obtenu en c. donne le résultat.

Partie 2

A.1. Il s'agit juste d'une identité remarquable :

$$b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + b^{n-3}a^2 + \cdots + ba^{n-2} + a^{n-1}).$$

A.2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si, et seulement si, tous les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles. D'après le rappel, cela est vrai si, et seulement si, les classes des nombres 1 à $n-1$ sont inversibles, ce qui, en vertu du rappel, est équivalent à dire que les nombres de 1 à $n-1$ sont premiers avec n. Ceci est donc vrai si, et seulement si, n est premier.

A.3.a. Si $k = 1$, P s'écrit $P(X) = X - \dot{a}$. $\dot{a}$ est la seule racine de P. Supposons le résultat vrai si P est de degré k, et prouvons-le pour P de degré $k+1$. Si P n'a pas de racines, le résultat est évident. Sinon, soit $\dot{a}$ une racine de P. On a la factorisation $P(X) = (X - \dot{a})Q(X)$ (que l'on peut obtenir, par exemple, en effectuant la division euclidienne de P par $X - \dot{a}$). Puisque $\mathbb{Z}/n\mathbb{Z}$ est un corps, les autres racines de P sont nécessairement des racines de Q qui est de degré $\leq k$. L'hypothèse de récurrence s'applique.

A.3.b. On a :

- $P(\dot{1}) = \dot{0}$.
- $P(\dot{2}) = \dot{2} \neq \dot{0}$.
- $P(\dot{3}) = \dot{6} = \dot{0}$.
- $P(\dot{4}) = \dot{12} = \dot{0}$.
- $P(\dot{5}) = \dot{2} \neq \dot{0}$.
- $P(\dot{0}) = \dot{0}$.

P admet 4 racines, à savoir $\dot{1}$, $\dot{3}$, $\dot{4}$ et $\dot{0}$: la propriété précédente n'est plus vraie si n n'est pas premier.

A.3.c. D'une part, on a $X^2 - X = X(X - \dot{1})$. D'autre part, on a :

$$(X - \dot{3})(X - \dot{4}) = X^2 - \dot{7}X + \dot{12} = X^2 - X.$$

A.4.a. Posons $H = \left\{1, x, \ldots, x^{k-1}\right\}$. Remarquons que $1 \in H$, et que si $x^a \in H$, avec $1 \leq a \leq k-1$, on a :

$$x^a x^{k-a} = x^{k-a}x^a = x^k = 1,$$

avec $x^{k-a} \in H$. En particulier, d'après le théorème de Lagrange, le cardinal de H, c'est-à-dire k, divise le cardinal de G. Ainsi, on peut écrire $n = km$, et on a $x^n = (x^k)^m = 1$.

A.4.b. Soit $G = (\mathbb{Z}/p\mathbb{Z})^*$, de cardinal $p-1$. D'après la question précédente, $\dot{x}^{p-1} = \dot{1}$. En particulier, $x^{p-1} - 1$ est divisible par p.

B.1. Pour $d \in D_{m-1}$, on note $H_d = \{x \in (\mathbb{Z}/n\mathbb{Z})^*;\ \text{ordre } x = d\}$. Les H_d forment une partition de $(\mathbb{Z}/n\mathbb{Z})^*$, et le cardinal de chaque H_d est d. On en déduit le résultat.

B.2.a. $X^d - \dot{1}$ admet au plus d racines, et chaque $\dot{a}^k$, pour $0 \leq k \leq d-1$, en est une. C'est donc que ce sont exactement les racines de $X^d - \dot{1}$.

B.2.b. Par hypothèse, $k = lu$ et $d = lv$, où $l \geq 2$ est le pgcd de k et d. On a alors :

$$(\dot{a}^k)^v = (\dot{a}^u)^{lv} = (\dot{a}^u)^d = \dot{1}.$$

L'ordre de $\dot{a}$ est donc inférieur ou égal à v, et est donc strictement inférieur ou égal à d.

B.2.c. On note toujours H_d l'ensemble des éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre d. D'après a.,

$$H_d \subset \left\{\dot{1}, \dot{a}, \dot{a}^2, \ldots, \dot{a}^{d-1}\right\}.$$

On note enfin

$$F = \left\{\dot{a}^k;\ 0 \leq k \leq d-1,\ k \wedge d \neq 1\right\}.$$

D'après b., $H_d \cap F = \varnothing$, et donc $\text{card}(H_d)+\text{card}(F) \leq d$. Maintenant, on sait que $\text{card}(F) = d-\phi(d)$, et que $\text{card}(H_d) = \zeta(d)$. Ceci entraine que $\zeta(d) \leq \phi(d)$.
Du fait que

$$\sum_{d\in D_{n-1}} \zeta(d) = \sum_{d\in D_{n-1}} \phi(d) = n-1,$$

on a obligatoirement $\zeta(d) = \phi(d)$ pour tout diviseur d de $n-1$. En particulier, $\zeta(n-1) = \phi(n-1) > 0$. Donc il existe au moins un élément $\dot{b}$ d'ordre $n-1$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Puisque :

- $\left\{\dot{1},\dot{b},\ldots,\dot{b}^{n-2}\right\} \subset (\mathbb{Z}/n\mathbb{Z})^*$.
- $\text{card}\left((\mathbb{Z}/n\mathbb{Z})^*\right) = n-1$.
- $\text{card}\left\{\dot{1},\dot{b},\ldots,\dot{b}^{n-2}\right\} = n-1$.

On en déduit donc que

$$(\mathbb{Z}/n\mathbb{Z})^* = \left\{\dot{1},\dot{b},\ldots,\dot{b}^{n-2}\right\}.$$

C.1. Supposons ces deux nombres congrus à 1 modulo p^2. On aurait alors :

$$(b+p)^{p-1} - b^{p-1} \equiv 0 \mod p^2,$$

ou encore :

$$\sum_{k=0}^{p-2} C_{p-1}^k b^k p^{p-1-k} \equiv 0 \mod p^2.$$

On coupe cette somme en deux :

$$\sum_{k=0}^{p-3} C_{p-1}^k b^k p^{p-1-k} + C_{p-1}^{p-2} b^{p-2} p \equiv 0 \mod p^2.$$

Maintenant, si k appartient à $\{0,\ldots,p-3\}$, p^2 divise p^{p-1-k}, et

$$\sum_{k=0}^{p-3} C_{p-1}^k b^k p^{p-1-k} \equiv 0 \mod p^2.$$

Finalement, on obtiendrait $p^2|(p-1)b^{p-2}p$, soit $p|(p-1)b^{p-2}$. Mais puisque $\dot{b}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$, il est impossible que $p|b^{p-2}$, et on aurait $p|p-1$. C'est bien sûr absurde!

C.2. Pour $r=0$, le résultat est prouvé : en effet, $c^{p-1} \equiv 1 \mod p$, donc $c^{p-1} = 1+k_0 p$, et puisque c^{p-1} n'est pas congru à 1 modulo p^2, $k_0 \wedge p = 1$.
Supposons maintenant le résultat prouvé au rang r, et prouvons-le au rang $r+1$. On a :

$$\begin{aligned} c^{p^{r+1}(p-1)} &= \left(c^{p^r(p-1)}\right)^p \\ &= \left(1+k_r p^{r+1}\right)^p \\ &= 1+k_r p^{r+2} + p^{r+3}u, \end{aligned}$$

où u est un entier (on a utilisé la formule du binôme, isolé les deux premiers termes, et regroupé les autres pour lesquels p^{2r+2} est en facteur). On en déduit :

$$c^{p^{r+1}(p-1)} = 1 + (k_r + pu) \times p^{r+2}.$$

Puisque k_r est premier avec p, il est clair que $k_{r+1} = k_r + pu$ est lui-aussi premier avec p (ils ont le même reste modulo p).
En particulier, si on applique le résultat à $r = \alpha - 1$, on obtient

$$\dot{c}^{p^{\alpha-1}(p-1)} = \dot{1}.$$

$\dot{c}$ est donc inversible dans $(\mathbb{Z}/n\mathbb{Z})$ muni de la multiplication, son inverse valant $\dot{c}^{p^{\alpha-1}(p-1)-1}$.

C.3.a. $p^\alpha(p-1)$ est le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z},\times)^*$. D'après la question A.4.a., $r|p^{\alpha-1}(p-1)$. D'autre part, $c^r \equiv 1 \mod p^\alpha \implies c^r \equiv 1 \mod p$. Mais la classe de $\dot{c}$ dans $(\mathbb{Z}/p\mathbb{Z},\times)^*$ est d'ordre $p-1$, et donc $p-1|r$.

C.3.b. r s'écrit $k(p-1)$, et $p^{\alpha-1}(p-1)$ d'écrit $k'r$. En particulier,

$$p^{\alpha-1}(p-1) = kk'(p-1) \implies k|p^{\alpha-1}.$$

Puisque p est premier, il existe $\beta \leq \alpha-1$ tel que $k = p^\beta$ et $r = p^\beta(p-1)$.

C.3.c. On utilise le résultat de la question 2 : si $\beta < \alpha-1$, $c^{p^\beta(p-1)}$ n'est pas congru à 1 modulo p^α. On a donc $\beta = \alpha-1$. Le groupe engendré par $\dot{c}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ est alors de cardinal $p^{\alpha-1}(p-1)$, ce qui est exactement le cardinal du groupe tout entier. C'est bien que $\dot{c}$ est générateur de $(\mathbb{Z}/n\mathbb{Z})^*$.
Remarquons ici l'usage de résultats pas vraiment démontrés avant, mais qui font partie du folklore mathématique et arithmétique, en particulier que l'ordre du sous-groupe engendré par un élément vaut l'ordre de cet élément. Il faut bien sûr considérer ce résultat comme du cours. Ce qui (me) gêne un peu, c'est que dans la question II.A.4., on démontre parfois des résultats que l'on peut considérer tout autant comme connus des candidats. Alors, qu'admettre, et que démontrer???

C.4. On cherche d'abord un générateur pour $(\mathbb{Z}/7\mathbb{Z})^*$. On a notamment :

k	1	2	3	4	5	6
$\dot{3}^k$	$\dot{3}$	$\dot{2}$	$\dot{6}$	$\dot{4}$	$\dot{5}$	$\dot{1}$

$\dot{3}$ est donc un générateur de $(\mathbb{Z}/7\mathbb{Z})^*$, et la question 1. prouve que ou $\dot{3}$ ou $\dot{10}$ est générateur de $(\mathbb{Z}/49\mathbb{Z})^*$. Mais :

$$3^6 = 729 = 43 + 14 \times 49.$$

3^6 n'est pas congru à 1 modulo 49, et donc $\dot{3}$ est générateur de $(\mathbb{Z}/49\mathbb{Z})^*$.

Partie 2

1.a. D'après le petit théorème de Fermat, dans $\mathbb{Z}/p\mathbb{Z}$,

$$\begin{aligned} & \dot{a}^{p-1} = 1 \\ \iff & \left(\dot{a}^{\frac{p-1}{2}}\right)^2 - \dot{1}^2 = 0 \\ \iff & \left(\dot{a}^{\frac{p-1}{2}} - 1\right)\left(\dot{a}^{\frac{p-1}{2}} + 1\right) = 0. \end{aligned}$$

Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, ceci entraîne que $a^{\frac{p-1}{2}}$ est congru à 1 ou -1 modulo p, ce qui est le résultat demandé (-1 est congru à $p-1$ modulo p).

1.b. Isolons d'abord le résultat suivant : si $r > 0$ est tel que $a^{q\times 2^r} \equiv 1 \mod p$, alors $a^{q\times 2^{r-1}} \equiv 1 \mod p$ ou $a^{q\times 2^{r-1}} \equiv p-1 \mod p$. La démonstration se fait exactement comme à la question précédente, en factorisant le polynôme X^2-1 dans $\mathbb{Z}/p\mathbb{Z}$.
Nous sommes alors prêts à prouver le résultat : si $a \wedge p = 1$, la question précédente entraîne que $a^{(p-1)\times 2^{s-1}}$ est congru à 1 ou $p-1$ modulo p. Si c'est le deuxième cas, alors a vérifie $H_a(p)$. Sinon, on a alors :

$$a^{(p-1)\times 2^{s-2}} \equiv 1 \text{ ou } p-1 \mod p.$$

Le cas $p-1$ règle le problème, sinon on itère le raisonnement : ou bien on trouve r, $0 \leq r < s$ tel que $a^{q\times 2^r} \equiv p-1 \mod p$ (et donc a vérifie $H_a(p)$). Ou bien, pour tout r, $0 \leq r < s$, on a $a^{q\times 2^r} \equiv 1 \mod p$. Mais faire $r = 0$ dans cette dernière hypothèse prouve aussi que a vérifie $H_a(p)$.

2. Soit $d = a \wedge p$, et supposons que $d > 1$. Si on avait $a^q \equiv 1 \mod p$, alors, puisque $d|a^q$ et $d|p$, on aurait $d|1$ ce qui est impossible puisque $d > 1$. De même, si on avait $a^{q \times 2^r} \equiv p - 1 \mod p$, on aurait $d| - 1$, ce qui est tout aussi impossible.

3.a. C'est la première fois qu'un problème du Capes demande d'écrire et d'implémenter un algorithme aussi compliqué. En cela, ce problème illustre bien deux tendances récentes : plus d'algorithmique, et plus de probabilités. Une des erreurs à ne pas faire concerne le calcul des exponentiel $a^q \mod p$. Il ne faut pas demander à la calculatrice de calculer a^q, puis de réduire modulo p. En effet, si on calcule par exemple 17^15, on obtient un nombre d'environ 18 chiffres, alors que la précision interne de la machine se limité à 12 chiffres. Faire la réduction modulo p se révèle alors absurde. Il faut au contraire réduire modulo p à chaque calcul de puissance! Voici une proposition d'algorithme :

```
/* Première étape : on cherche les nombres q et s */
0->s
p-1->b
Tant que b/2=[b/2], faire  /*[x] désigne la partie entière de x*/
  s+1->s
  b/2->b
Fin Tant que.
(p-1)/2^s->q
1->b
/*On calcule a^q*/
Pour i de 1 à q faire (b*a) mod p ->b Fin Pour.
Si b=1, alors Afficher ‘‘p est a-ppf’’. Fin du Programme.
0->r
Tant que r<s, faire
  Si b=p-1, alors Afficher ‘‘p est a-ppf’’. Fin du Programme.
  b^2 mod p->b
  r+1->r
Fin Tant que.
/* Si on arrive ici, c'est que tous les tests précédents ont échoué*/
Afficher ‘‘p n'est pas a-ppf’’.
Si
```

2^a

3.b. Le programme précédent a renvoyé les résultats suivants :

p	49	91	11	121	135	1225
a	30	74	28	94	43	999
$p$est $a-$ ppf	oui	oui	non	oui	non	oui

3.c. On a le tableau suivant :

k		1	2	3	4	5	6	7	8	9	10
50^k	mod 561	50	256	458	460	560	511	305	103	101	1

Le sous-groupe cyclique de $((\mathbb{Z}/561\mathbb{Z})^*, \times)$ engendré par $\dot{50}$ est exactement l'ensemble demandé.

Partie 2

A.1. D'abord, un tel nombre n'est pas premier (on suppose bien sûr, ce qui n'est pas dit explicitement dans l'énoncé, que $k \geq 2$). D'autre part, si a est premier avec n, on sait que a est premier avec

chacun des p_i et le petit théorème de Fermat a pour conséquence l'égalité $a^{p_i-1} \equiv 1 \mod p_i$. Mais $n-1 = q_i(p_1-1)$, et donc on a $a^{n-1} \equiv 1 \mod p_i$. On a donc, pour $i = 1,2,\ldots,k$, $p_i | a^{n-1}-1$. Comme les p_i sont premiers entre eux deux à deux, on a $p_1 \ldots p_k | a^{n-1}-1$, et donc $a^{n-1} \equiv 1 \mod n$ (ce qui peut aussi se retrouver par le théorème chinois). Un tel nombre est donc un nombre de Carmichael.

On a :

$$561 = 3 \times 11 \times 17,$$

et il est aisé de vérifier que 2, 10 et 16 divisent 560. De même,

$$10585 = 5 \times 29 \times 73,$$

et il est aisé de vérifier que 4, 28 et 72 divisent 10584.

A.2.a. D'après les résultats de la partie I, le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$ est $\phi(2^\alpha) = 2^{\alpha-1}$. Soit a un entier impair, et r l'ordre de $\dot{a}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Si $a^{2^\alpha-1}$ était congru à 1 modulo n, on aurait $r | 2^\alpha - 1$. Mais r divise aussi l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^*$, et donc r est une puissance de 2, $r = 2^k$. Mais la condition $2^k | 2^\alpha - 1$ force k à être nul. Par conséquent, a est congru à 1 modulo n.

Ainsi, puisque $\alpha \geq 2$, si l'on prend $a = 3$, a n'est pas congru à 1 modulo n, et a^{n-1} n'est donc pas congru à 1 modulo n : n n'est pas un nombre de Carmichael.

A.2.b.i. On pose $p = p_1^{\alpha_1}$, $q = p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, et h la bijection de S_{pq} sur $S_p \times S_q$ définie à la question I.4. Soit t tel que $h(t) = (\omega,1)$. Par définition de h, $t \equiv \omega \mod p_1^{\alpha_1}$ et $t \equiv 1 \mod p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. En particulier, pour chaque i de $\{2,\ldots,k\}$, $t \equiv 1 \mod p_i^{\alpha_i}$. Ainsi, t est premier avec chacun des $p_i^{\alpha_i}$ et donc t est premier avec n. Puisque n est un nombre de Carmichael, $t^{n-1} \equiv 1 \mod n$.

A.2.b.ii. Soit $r \geq 1$ tel que $t^r \equiv 1 \mod n$. D'après le théorème des restes chinois, ceci est équivalent au système :

$$\begin{cases} t^r & \equiv & 1 & \mod p_1^{\alpha_1} \\ t^r & \equiv & 1 & \mod p_2^{\alpha_2} \\ \vdots & \vdots & \vdots & \\ t^r & \equiv & 1 & \mod p_r^{\alpha_r} \end{cases}$$

Mais, pour $i \geq 2$, les équations $t^r \equiv 1 \mod p_i^{\alpha_i}$ sont triviales, puisque l'on sait déjà que $t \equiv 1 \mod p_i^{\alpha_i}$. Par conséquent, on a l'équivalence :

$$t^r \equiv 1 \mod n \iff \omega^r \equiv 1 \mod p_1^{\alpha_1}.$$

Etant donné le choix de ω, ceci entraine que $p_1^{\alpha_1-1}(p-1)$ divise r. En particulier, on a obtenu que $p_1^{\alpha_1-1}(p-1)$ divise $n-1$. Si $\alpha_1 \geq 2$, on a donc $p_1 | n-1$ ce qui est impossible puisqu'on a aussi $p_1 | n$. C'est donc que $\alpha_1 = 1$, et que $p_1 - 1 | n-1$.

A.2.b.iii. $p_1 - 1$ est un nombre pair, et donc $2 | n-1$. En particulier, n est impair, et chacun des p_i est impair. Le raisonnement précédent peut leur être appliqué, ce qui prouve que pour chaque i $\alpha_i = 1$ et $p_i - 1$ divise $n-1$.

On a donc prouvé l'équivalence :

> n est un nombre de Carmichael si, et seulement si, $n = p_1 \times \cdots \times p_k$, où les p_i sont des nombres premiers deux à deux distincts tels que $p_i - 1$ divise $n-1$.

A.3. Supposons que n soit un nombre de Carmichael n'admettant que deux facteurs premiers distincts, $n = p_1 p_2$. On peut alors écrire $p_1 p_2 - 1 = k(p_1 - 1)$, ce qui se réécrit en :

$$p_2(p_1-1) + p_1 - 1 = k(p_1-1).$$

Ainsi, $p_1 - 1 | p_2 - 1$. Par symétrie, $p_2 - 1 | p_1 - 1$, et $p_1 = p_2$: c'est absurde!

A.4. Remarquons que $85 \wedge 16 = 1$, et donc par le théorème de Bézout, cette équation admet bien des solutions. On recherche une solution particulière en utilisant l'algorithme d'Euclide étendu. On obtient par exemple que $13 \times 85 - 69 \times 16 = 1$. Maintenant, si $85p - 16k = 1$, on a en retranchant la

solution particulière $85(p-13)-16(k-69)=0$. On a donc $16|85(p-13)$, et puisque $16\wedge 85=1$, on obtient $p=13+16m$, où m est un entier. Réintroduisant cela dans l'équation, on obtient :

$$85\times 13+16\times 85m-16k=1 \implies k=69+85m.$$

(k,p) est donc solution si, et seulement si, il existe m dans $\mathbb{Z}$ tel que $p=13+16m$ et $k=69+85m$. Appliquons ce résultat à la recherche du plus petit nombre de Carmichaël divisible par 5 et 17. On suppose qu'il s'écrit à l'aide de 3 facteurs premiers : $n=p\times 5\times 17$. Par les résultats précédents, $16|n-1$. Il existe donc k tel que $16k=85p-1$. Le plus petit nombre premier qui peut être solution de cette équation est 13, comme l'étude précédente l'a montré. Le plus petit nombre de Carmichaël divisible par 5 et 17, et possédant 3 facteurs premiers, est donc $13\times 5\times 17=1105$. Prouvons que c'est le plus petit nombre de Carmichaël divisible par 5 et 17. Si n' était un autre nombre de Carmichaël divisible par 5 et 17, et inférieur à 1105, il comporterait nécessairement au moins 4 facteurs premiers : $n'=5\times 17\times q_1\times q_2\times\cdots\times q_l$. On aurait alors $q_3\geq 3$ et $q_2\geq 7$, puisque les nombres premiers sont distincts, et donc $n'\geq 3\times 5\times 7\times 17=1785>1105$.
1105 est en fait le deuxième nombre de Carmichaël, après 561, les suivants étant 1729 et 2465. On sait depuis 1994 simplement qu'il existe une infinité de nombres de Carmichaël.

B.1. Puisque n n'est ni premier, ni un nombre de Carmichaël, il existe $a\leq n$ tel que $a^{n-1}\equiv 1 \mod n$. On fait l'hypothèse que n est impair (ce n'est pas écrit explicitement dans l'énoncé...) : la définition de fortement pseudo-premier n'est donnée que dans ce cadre, et de toute façon tester la primalité d'un nombre pair est assez peu intéressant. On écrit donc $n-1=q\times 2^s$, avec q impair. Si n n'était pas $a-$pff, ou bien $a^q\equiv 1 \mod n$, mais alors $a^{n-1}\equiv 1 \mod n$: impossible! Ou bien $a^{q\times 2^r}\equiv -1 \mod n$, avec $r<s$, ce qui entraîne $a^{q\times 2^{r+1}}\equiv 1 \mod n$, et ainsi $a^{n-1}\equiv 1 \mod n$, ce qui est toujours aussi impossible!

B.2. Soit $H=\{1\leq a\leq n; a\wedge n=1$ et nn'est pas a-pff$\}$. H est un sous-groupe strict d'un groupe de cardinal $\phi(n)$, son cardinal est inférieur à $\phi(n)/2\leq n/2$. Pour chaque épreuve, il y a donc une probabilité inférieure à $1/2$ de déclarer un nombre $a-$ppf s'il est composé. Les épreuves étant supposées indépendantes, la probabilité de déclarer n premier alors qu'il est composé après k épreuves peut être majorée par $(1/2)^k$.