Deuxième épreuve CAPES 2003

François Sauvageot

7 février 2003

Partie I

Question I.1.a

Puisque $(A_1, \overline{A}_1)$ forme une partition de Ω, $(A_1 \cap A_2, \overline{A}_1 \cap A_2)$ forme une partition de A_2. Il en résulte

$$\mathbf{P}(A_1) + \mathbf{P}(\overline{A}_1) = \mathbf{P}(\Omega) = 1 \qquad \text{et} \qquad \mathbf{P}(A_1 \cap A_2) + \mathbf{P}(\overline{A}_1 \cap A_2) = \mathbf{P}(A_2)$$

et donc, par indépendance de A_1 et A_2,

$$\mathbf{P}(\overline{A}_1 \cap A_2) = \mathbf{P}(A_2) - \mathbf{P}(A_1 \cap A_2) = \mathbf{P}(A_2) - \mathbf{P}(A_1)\mathbf{P}(A_2) = \mathbf{P}(A_2).(1 - \mathbf{P}(A_1)) = \mathbf{P}(A_2)\mathbf{P}(\overline{A}_1)\ .$$

Par conséquent $\overline{A}_1$ et A_2 sont indépendants.

Question I.1.b.I

Notons $X_1 = \overline{A}_1$ et, pour j entier compris entre 2 et k, $X_j = A_j$. Soit J une partie de $\{1, \ldots, k\}$. Si J ne contient pas 1, par indépendance mutuelle de A_1, ..., A_k, on a

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

Si maintenant 1 appartient à J, notons $J' = J \setminus \{1\}$. Par indépendance mutuelle de A_1, ..., A_k, A_1 est indépendant de $\cap_{j\in J'} A_j$ et donc, d'après I.1.a, $\overline{A}_1$ est indépendant de $\cap_{j\in J'} A_j$. Il vient donc

$$\mathbf{P}\left(\cap_{j\in J} X_j\right) = \mathbf{P}\left(\overline{A_1} \cap \left(\cap_{j\in J'} A_j\right)\right) = \mathbf{P}(\overline{A_1})\mathbf{P}\left(\cap_{j\in J'} A_j\right) = \mathbf{P}(\overline{A_1}) \prod_{j\in J'} \mathbf{P}(A_j) = \prod_{j\in J} \mathbf{P}(X_j)\ .$$

Il en résulte que X_1, ..., X_k sont mutuellement indépendants, i.e. $\overline{A}_1$, A_2, ..., A_k sont mutuellement indépendants.

Question I.1.b.II

Pour j un entier compris entre 0 et k, soit (H_j) la propriété : si des évènements X_1, ..., X_k sont des évènements mutuellement indépendants de B, alors les évènements $\overline{X}_i$, pour i entier tel que $1 \leq i \leq j$, et X_ℓ, pour ℓ entier tel que $j < \ell \leq k$, sont mutuellement indépendants.

La propriété (H_0) est une tautologie, et (H_1) est vraie d'après ce qui précède.

Soit j un entier compris entre 0 et $k-1$ tel que (H_j) soit vraie. En appliquant I.1.b.I aux évènements X_{j+1}, $\overline{X}_1$, ..., $\overline{X}_j$, X_{j+2}, ..., X_k, on en déduit que H_{j+1} est vraie.

Par conséquent le principe de récurrence entraîne que (H_j) est vraie pour tout entier j compris entre 0 et k. En particulier (H_k) l'est, ce qui est exactement l'assertion recherchée.

Question I.2.a

Notons T l'ensemble $\{1, \ldots, n\}$. Puisque la loi de X est uniforme sur T, pour tout sous-ensemble T' de T, on a $\mathbf{P}(X \in T') = Card(T')/\,Card(T)$. Notons $T_2 = T \cap 2\mathbf{N}$ et $T_5 = T \cap 5\mathbf{N}$. Puisque 2 et 5 sont premiers entre eux, leur ppcm est 10 et

donc un entier est divisible par 2 et 5 si et seulement si'l est divisible par 10. Il en résulte $T_2 \cap T_5 = T \cap (2\mathbf{N} \cap 5\mathbf{N}) = T \cap 10\mathbf{N}$. Nous noterons T_{10} ce dernier ensemble. On a donc

$$\mathbf{P}(A_1) = \mathbf{P}(X \in T_2) = \frac{Card\, T_2}{Card\, T}\ , \qquad \mathbf{P}(A_2) = \mathbf{P}(X \in T_5) = \frac{Card\, T_5}{Card\, T}\ , \quad \text{et} \quad \mathbf{P}(A_1 \cap A_2) = \mathbf{P}(X \in T_2 \cap T_5) = \frac{Card\, T_{10}}{Card\, T}\ .$$

Par conséquent si $n = 100$, on a

$$\mathbf{P}(A_1) = \frac{50}{100} = \frac{1}{2}\ , \qquad \mathbf{P}(A_2) = \frac{20}{100} = \frac{1}{5}\ , \qquad \text{et} \quad \mathbf{P}(A_1 \cap A_2) = \frac{10}{100} = \frac{1}{10}\ .$$

En particulier A_1 et A_2 sont indépendants.

Question I.2.b

Si l'on fait $n = 101$ dans les calculs précédents, comme 101 est premier à 2, 5 et 10, les cardinaux de T_2, T_5 et T_{10} sont inchangés et il vient

$$\mathbf{P}(A_1) = \frac{50}{101}\ , \qquad \mathbf{P}(A_2) = \frac{20}{101}\ , \qquad \text{et} \quad \mathbf{P}(A_1 \cap A_2) = \frac{10}{101}$$

et donc

$$\mathbf{P}(A_1)\mathbf{P}(A_2) = \mathbf{P}(A_1 \cap A_2) \Leftrightarrow 50 \times 20 = 10 \times 101 \Leftrightarrow 1000 = 1010\ ,$$

ce qui montre que A_1 et A_2 ne sont pas, cette fois-ci, indépendants.

Question I.3.a

L'évènement A est l'évènement $X \in S_n$ et donc $\mathbf{P}(A) = Card\, S_n / Card\, T$, i.e. $\mathbf{P}(A) = \varphi(n)/n$.

Question I.3.b

Soit p un entier naturel, notons $T_p = T \cap p\mathbf{N}$. Si p est un diviseur de n, on peut écrire $n = pd$ avec d entier, de sorte que T_p est l'ensemble des multiples de p s'écrivant mp avec m entier compris entre 1 et d. En particulier T_p est de cardinal d, c'est-à-dire n/p et donc $\mathbf{P}(X \in T_p) = 1/p$.

Il vient, pour tout entier i compris entre 1 et k, puisque p_i est un diviseur de n,

$$\mathbf{P}(A_i) = \mathbf{P}(X \in T_{p_i}) = \frac{1}{p_i}\ .$$

Question I.3.c

Soit J une partie de $\{1, \ldots, k\}$. Comme $(p_j)_{j \in J}$ sont des nombres premiers distincts, ils sont premiers entre eux et donc leur ppcm est $\prod_{j \in J} p_j$. Il en résulte $\cap_{j \in J} p_j \mathbf{N} = \prod_{j \in J} p_j \mathbf{N}$ et donc $\cap_{j \in J} T_{p_j} = T \cap \prod_{j \in J} p_j \mathbf{N}$. De plus $\prod_{j \in J} p_j$ est un diviseur de n et il vient

$$\mathbf{P}(\cap_{j \in J} A_j) = \mathbf{P}(X \in \cap_{j \in J} T_{p_j}) = \mathbf{P}(X \in T_{\prod_{j \in J} p_j}) = \frac{1}{\prod_{j \in J} p_j} = \prod_{j \in J} \frac{1}{p_j} = \prod_{j \in J} \mathbf{P}(A_j)$$

et donc les évènements A_1, A_2, …, A_k sont mutuellement indépendants.

Question I.3.d

Soit m un entier. S'il n'est pas premier à n, c'est que n et m ont un diviseur commun et donc, puisque tout nombre est produit de facteurs premiers, n et m ont un diviseur premier en commun. Autrement dit, il existe un entier i compris entre 1 et k tel que p_i divise m. Par conséquent l'évènement A se produit si et seulement aucun des évènements A_i ne se produit, i.e. $A = \overline{A}_1 \cap \ldots \cap \overline{A}_k$.

Question I.3.e

Il résulte des deux questions précédentes et de I.1.b.II

$$\mathbf{P}(A) = \mathbf{P}(\overline{A}_1 \cap \ldots \cap \overline{A}_k) = \prod_{i=1}^{k} \mathbf{P}(\overline{A}_i) = \prod_{i=1}^{k} (1 - \mathbf{P}(A_i)) = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) .$$

Comme, d'après I.3.a, $\mathbf{P}(A) = \varphi(n)/n$, il vient

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) .$$

Question I.4.a

Soit r dans S_{pq} et (a, b) son image par h. D'après les propriétés de la division euclidienne, on a en particulier $PGCD(r, p) = PGCD(p, a)$ et $PGCD(r, q) = (q, b)$. Or, r appartient à S_{pq} et donc r est premier à pq et donc à p et q. Il en résulte

$$PGCD(p, a) = PGCD(r, p) = 1 = PGCD(r, q) = PGCD(q, b) ,$$

i.e. a appartient à S_p et b à S_q. Autrement dit (a, b) appartient à $S_p \times S_q$ et donc $h(S_{pq})$ est inclus dans $S_p \times S_q$.

Question I.4.b

Soit x et y dans S_{pq} tels que $h(x) = h(y) = (a, b)$. En particulier

$$x \equiv a \equiv y \ mod\ p \qquad \text{et} \qquad x \equiv b \equiv y \ mod\ q,$$

et donc p et q divisent $x - y$. Comme p et q sont premiers entre eux, il en résulte que pq divise $x - y$. Or x et y vérifient $0 \leq x, y < pq$ et donc $|x - y| < pq$. On en déduit $x - y = 0$ ou encore $x = y$. Par conséquent h est injective.

Question I.4.c

Puisque p et q sont premiers entre eux, on peut trouver une relation de Bézout entre eux, i.e. il existe deux entiers relatifs α et β tels que $\alpha p + \beta q = 1$.

Soit donc α et β deux tels entiers, (a, b) dans $S_p \times S_q$ et x donné par $x = \alpha pb + \beta qa$. La relation $\alpha p + \beta q = 1$ entraîne en particulier $\alpha p \equiv 1 \ mod\ q$ et $\beta q \equiv 1 \ mod\ p$ et il vient

$$x \equiv 0.b + 1.a \equiv a \ mod\ p \qquad \text{et} \qquad x \equiv 1.b + 0.a \equiv b \ mod q .$$

Soit r le reste de la division euclidienne de x par pq, on a donc $0 \leq r < pq$, $r \equiv a \ mod\ p$ et $r \equiv b \ mod q$. Des deux dernières propriétés et du fait que (a, b) appartient à $S_p \times S_q$, on en déduit que r est premier à p et q. Il est donc premier à pq. En particulier r est non nul. Au final r est un entier vérifiant $0 < r < pq$ et premier à pq, i.e. r appartient à S_{pq}.

Au final, pour tout couple (a, b) de $S_p \times S_q$, on a exhibé un élément r de S_{pq} tel que $h(r) = (a, b)$. Par conséquent l'image de h est $S_p \times S_q$.

Comme h est injective, d'après la question précédente, h induit une bijection entre S_{pq} et son image, i.e.$S_p \times S_q$. Comme ce sont deux ensembles finis, l'existence d'une bijection entre eux entraîne qu'ils ont même cardinaux, i.e. $\varphi(pq) = \varphi(p)\varphi(q)$.

Question I.4.d

Pour k entier naturel, notons (H_k) la propriété : pour tout k-uplet $(p_1, \ldots, p_k)$ de nombres premiers distincts et tout k-uplet $(\alpha_1, \ldots, \alpha_k)$ d'entiers naturels non nuls, on a

$$\varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) .$$

Soit p un nombre premier, α un entier naturel non nul et m un entier naturel compris entre 1 et p^α. Les diviseurs de p^α sont les p^β avec β entier vérifiant $0 \leq \beta \leq \alpha$. Par conséquent le pgcd de m et p^α est nécessairement de cette forme. Il

en résulte que m et p^α sont premiers entre eux si et seulement si p ne divise pas m. Les multiples de p compris entre 1 et p^α étant les nombres de la forme $p\ell$ avec $1 \leq \ell \leq p^{\alpha-1}$, ils sont au nombre de $p^{\alpha-1}$. Il en résulte que S_p est de cardinal $p^\alpha - p^{\alpha-1}$, i.e. $\varphi(p^\alpha) = p^\alpha(1-1/p)$.

Par conséquent (H_1) est vraie.

Soit maintenant k un entier naturel non nul, $(p_1, \ldots, p_{k+1})$ un $(k+1)$-uplet de nombres premiers distincts et $(\alpha_1, \ldots, \alpha_{k+1})$ un $(k+1)$-uplet de nombres entiers naturels non nuls. D'après la question précédente, on a

$$\varphi\left(\prod_{i=1}^{k+1} p_i^{\alpha_i}\right) = \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)\varphi(p_{k+1}^{\alpha_{k+1}}) = \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) p_{k+1}^{\alpha_{k+1}}\left(1-\frac{1}{p_{k+1}}\right)$$

et donc la propriété (H_k) est héréditaire.

D'après le principe de récurrence, la propriété (H_k) est donc vraie pour tout entier naturel non nul k. Comme n peut s'écrire, de façon unique, comme produit de puissances de nombres premiers distincts, on en déduit (E).

Question I.5.a

Pour d entier naturel non nul, notons G_d l'ensemble des entiers compris entre 1 et n dont le PGCD avec n est d.

Soit x, y, d trois entiers naturels non nuls, on a $PGCD(dx, dy) = d.PGCD(x, y)$. Par conséquent, si a est un entier naturel non nul, on a

$$PGCD(a,n) = d \Leftrightarrow d \mid n\ , d \mid a \ \text{ et } \ PGCD\left(\frac{a}{d}, \frac{n}{d}\right) = 1$$

et donc, si de plus d est un diviseur de n,

$$PGCD(a,n) = d \Leftrightarrow d \mid a \quad \text{et} \quad PGCD\left(\frac{a}{d}, \frac{n}{d}\right) \Leftrightarrow \exists k \in \mathbf{N} \quad a = kd \quad \text{et} \quad PGCD(k, \frac{n}{d}) = 1\ ,$$

ce qui est l'assertion recherchée.

Par conséquent, G_d est l'ensemble des entiers de la forme kd pour k entier naturel non nul inférieur à n/d et premiers avec n/d, i.e. pour k dans $S_{n/d}$. En particulier le nombre d'entiers a tels que $1 \leq a \leq n$ et $PGCD(a,n) = d$ est égal à $\varphi(n/d)$.

Question I.5.b

D'après la question précédente, on a

$$\mathbf{P}(C_d) = \frac{Card\, G_d}{Card\, T} = \frac{1}{n}\varphi\left(\frac{n}{d}\right)\ .$$

Question I.5.c

Puisque tout nombre compris entre 1 et n admet pour PGCD avec n un diviseur de n, la famille $(G_d)_{d\in D_n}$ recouvre T. De plus le PGCD de deux nombres est unique, et donc cette famille est en fait une partition de T.

D'après la formule des probabilités totales, il vient

$$1 = \mathbf{P}(X \in T) = \sum_{d\in D_n} \mathbf{P}(X \in G_d) = \sum_{d\in D_n} \mathbf{P}(C_d)$$

et donc

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

Question I.5.d

Soit d un diviseur de n, la quantité n/d est alors un entier et il vérifie $n = d.n/d$ et, en particulier, c'est un diviseur de n. Autrement dit on peut définir une application u de D_n dans lui-même par la formule $u(d) = n/d$.

Comme u est involutive, u est bijective.

Il vient

$$n = \sum_{d\in D_n} \varphi(u(d)) = \sum_{u(d)\in D_n} \varphi(u(d)) = \sum_{d'\in D_n} \varphi(d')$$

ce qui est l'assertion recherchée.

Partie II

Question II.A.1

Pour a et b dans A et n entier naturel non nul, on a

$$b^n - a^n = (b-a)\sum_{k=0}^{n-1} a^k b^{n-1-k}$$

et donc $b^n - a^n$ est divisible par $b-a$.

Il est raisonnable de penser que l'énoncé amène à penser que le quotient de $b^n - a^n$ par $b-a$ est égal à

$$\sum_{k=0}^{n-1} a^k b^{n-1-k}\ .$$

Remarque : Mais attention, dans un anneau général, il n'y a pas de notion de quotient. Ainsi demander « LE » quotient est ridicule. Prenons par exemple $A = \mathbf{Z}/8\mathbf{Z}$, a la classe de 2, b celle de 4 et $n = 2$. Alors $b^2 - a^2$ est la classe de 4 et $b-a$ celle de 2. Mais on a

$$\dot{4} = \dot{2}\times\dot{2} = \dot{2}\times\dot{6}$$

alors qu'est-ce que « LE » quotient de $b^2 - a^2$ par $b-a$? Pour que cela ait un sens précis, il faudrait supposer $b-a$ inversible dans A, mais ce n'est pas ce que veut l'énoncé (voir II.A.3.a).

Question II.A.2

Si n est un entier composé, on a $n = pq$ avec p et q deux entiers naturels strictement supérieurs à 1. Et comme $p \mid n$ et $q \mid n$, p et q vérifient en fait $1 < p, q < n$. En particulier leurs classes modulo n est non nulle.

Or $n = pq$ et donc la classe de pq est nulle, autrement dit la multiplication dans $\mathbf{Z}/n\mathbf{Z}$ de la classe de p par celle de q donne la classe nulle. En particulier l'anneau $\mathbf{Z}/n\mathbf{Z}$ n'est pas intègre et ne saurait donc être un corps.

Si maintenant a est un entier premier à n, on a une relation de Bézout entre a et n. Soit donc α et β deux entiers relatifs tels que $\alpha a + \beta n = 1$. En particulier $\alpha a \equiv 1\ mod\ n$. Il en résulte que la classe de a dans $\mathbf{Z}/n\mathbf{Z}$ est inversible et admet la classe de α comme inverse. En particulier si n est premier, ce résultat est valable pour tout entier dont la classe modulo n n'est pas nulle, i.e. $\mathbf{Z}/n\mathbf{Z}$ est un corps.

Ainsi, $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est premier.

Remarque : On pourrait aussi utiliser l'affirmation de l'énoncé. En effet $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si tous ses éléments non nuls sont inversibles et donc si et seulement si le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$ est $n-1$, i.e. si et seulement si $\varphi(n) = n-1$. Mais d'après (E) (voir I.3.e), on a

$$\varphi(n) = n-1 \Leftrightarrow \prod_{p|n}\left(1-\frac{1}{p}\right) = 1-\frac{1}{n}$$

où le produit est étendu sur tous les nombres premiers p divisant n. Maintenant tous les termes du produit sont inférieurs à $1-1/n$ et aussi strictement inférieurs à 1. Il ne peut donc y avoir qu'un seul terme dans le produit et ce terme doit être $1-1/n$, i.e. n doit être premier !

Question II.A.3.a

Remarque : Bien entendu la théorie des anneaux de polynômes sur un anneau ou sur un corps autre qu'un sous-corps de $\mathbf{C}$ est hors-programme et aucun résultat provenant de cette théorie ne peut être appliqué ici. Il faut donc utiliser d'autres méthodes. La plus naturelle consiste tout simplement à utiliser les deux questions précédentes. D'ailleurs pourquoi sinon avoir posé la question II.A.1 ?

Soit donc n un entier premier et K le corps $\mathbf{Z}/n\mathbf{Z}$.

Pour k entier naturel, notons (H_k) la propriété : un polynôme de degré k à coefficients dans $\mathbf{Z}/n\mathbf{Z}$ admet au plus k racines dans $\mathbf{Z}/n\mathbf{Z}$. Autrement dit, si $(a_0, \ldots, a_k)$ sont $k+1$ éléments de K avec a_k non nul, alors la fonction polynôme de K dans K définie par

$$x \mapsto a_0 + a_1 x + \ldots + a_k x^k$$

s'annule au plus k fois.

La propriété (H_0) est vraie puisqu'une fonction polynôme associée à un polynôme de degré 0 est une fonction constante non nulle et donc ne s'annule pas.

Soit maintenant k un entier naturel, $(a_0, \ldots, a_{k+1})$ $k+2$ éléments de K et P une fonction polynôme de K dans K définie par

$$x \mapsto a_0 + a_1 x + \ldots + a_{k+1} x^{k+1} \ .$$

Soit α dans K tel que $P(\alpha) = 0$ et x dans K. On a

$$P(x) = 0 \Leftrightarrow P(x) - P(\alpha) = 0 = \Leftrightarrow \sum_{j=1}^{k+1} a_j (x^j - \alpha^j) = 0 \Leftrightarrow (x-\alpha) \sum_{j=1}^{k+1} \sum_{\ell=0}^{j-1} a_j \alpha^{j-1-\ell} x^\ell = 0$$

et donc, par intégrité de K et en permutant les deux sommes (par associativité et commutativité de K),

$$P(x) = 0 \Leftrightarrow \left(x = \alpha \quad \text{ou} \quad \sum_{\ell=0}^{k} \left(\sum_{j=\ell+1}^{k+1} a_j \alpha^{j-1-\ell} \right) x^\ell = 0 \right) \ .$$

Autrement dit toute racine de P distincte de α est racine d'un certaine fonction polynôme associée à un polynôme de degré k. La propriété (H_k) est donc héréditaire.

Le principe de récurrence permet donc de conclure que (H_k) est vraie pour tout entier naturel. En particulier pour k entier non nul, tout « polynôme » de degré k à coefficients dans $\mathbf{Z}/n\mathbf{Z}$ admet au plus k racines.

Remarque : Comme les polynômes à coefficients dans $\mathbf{Z}/n\mathbf{Z}$ ne sont pas au programme, il me semble plus légitime de parler de « fonction polynôme », ce qui a toujours un sens. Par contre le degré d'une telle fonction est plus ambigü, puisque par exemple la fonction nulle est également la fonction polynôme $X^n - X$ lorsque n est premier (voir II.A.4.b).

Question II.A.3.b

On vérifie directement (par exemple sur calculatrice, mais aussi sur papier) qu'on a

$$P(\dot{0}) = P(\dot{1}) = P(\dot{3}) = P(\dot{4}) = \dot{0} \qquad \text{et} \qquad P(\dot{2}) = P(\dot{5}) = \dot{2}$$

et donc les racines de P sont $\dot{0}$, $\dot{1}$, $\dot{3}$ et $\dot{4}$.

Question II.A.3.c

On a

$$X(X-\dot{1}) = X^2 - \dot{1}X = X^2 - X \quad \text{et} \quad (X-\dot{3})(X-\dot{4}) = X^2 - (\dot{3}+\dot{4})X + \dot{3}\dot{4} = X^2 - \dot{1}X + \dot{0} = X^2 - X \ .$$

Par conséquent $X(X-\dot{1})$ et $(X-\dot{3})(X-\dot{4})$ sont deux factorisations distinctes de P dans $\mathbf{Z}/6\mathbf{Z}[X]$.

Remarque : Depuis la question précédente, $\mathbf{Z}/6\mathbf{Z}[X]$ n'est toujours pas au programme !

Question II.A.4.a

Notons H l'ensemble $\{1, x, \ldots, x^{k-1}\}$. Remarquons que H n'est pas vide puisqu'il contient 1.

Soit ℓ un entier relatif et q et r les quotients et restes de la division euclidienne de ℓ par k. L'élément x^ℓ appartient à G puisque G est un groupe et on a

$$x^\ell = x^{qk+r} = (x^k)^q x^r = 1^q x^r = x^r$$

et donc x^ℓ appartient à H. De plus comme k est l'ordre de x et comme $0 \leq r < k$, x^r n'est égal à 1 que si r est nul. C'est-à-dire que x^ℓ est égal à 1 si et seulement si ℓ est divisible par k.

Par conséquent si i et j sont deux entiers naturels inférieurs strictement à k, comme $i-j$ est un entier, x^{i-j} appartient à H. Autrement dit $x^i(x^j)^{-1}$ appartient à H. Par conséquent pour tout (x, y) dans H^2, xy^{-1} appartient à H et il en résulte, avec le fait que H est non vide, que H est un sous-groupe de G, i.e. $\{1, x, \ldots, x^{k-1}\}$ est un sous-groupe de G.

Remarquons maintenant H est formé d'éléments distincts. En effet si i et j sont deux entiers naturels inférieurs strictement à k, on a $x^i = x^j$ si et seulement si $x^{i-j} = 1$ et donc si et seulement si k divise $i-j$. Comme $0 \leq i, j < k$, on a $|i-j| < k$, et donc $x^i = x^j$ si et seulement si $i = j$. Par conséquent H est un sous-groupe de G de cardinal k. D'après le théorème de Lagrange, le cardinal de H divise celui de G, i.e. k divise n, ou encore : l'ordre de tout élément de G divise le cardinal de G.

En particulier n est divisible par k et la remarque précédente montre que x^n est égal à 1.

Question II.A.4.b

Soit p un nombre premier et G le groupe $(\mathbf{Z}/p\mathbf{Z})^*$. Puisque $\varphi(p)$ est égal à $p-1$ ou encore puisque $\mathbf{Z}/p\mathbf{Z}$ est un corps, le cardinal de G est $p-1$ et donc, pour tout élément a de G, on a $a^{p-1} = \dot{1}$.

Soit maintenant x un entier naturel non divisible par p. D'après la propriété rappelée par l'énoncé, la classe de x est inversible dans $\mathbf{Z}/p\mathbf{Z}$ et donc $\dot{x}$ appartient à G. Il en résulte $\dot{x}^{p-1} = \dot{1}$ ou encore $x^{p-1} = 1 \; mod \; p$, soit encore : $x^{p-1} - 1$ est divisible par p.

Remarque : Ce résultat est connu comme le petit théorème de Fermat, mais ce théorème est hors-programme et il n'est donc pas licite de l'utiliser.

Question II.B.1

Puisque n est premier, $\mathbf{Z}/n\mathbf{Z}$ est un corps d'après II.A.2 et donc $(\mathbf{Z}/n\mathbf{Z})^*$ est de cardinal $n-1$.

D'après II.A.4.a l'ordre de tout élément de $(\mathbf{Z}/n\mathbf{Z})^*$ divise le cardinal de ce groupe, i.e. appartient à D_{n-1}. De plus tout élément de $(\mathbf{Z}/n\mathbf{Z})^*$ admet un ordre et un seul, par définition, et donc les ensembles formés des éléments d'ordre d, pour d dans D_{n-1}, forment une partition de $(\mathbf{Z}/n\mathbf{Z})^*$. Il en résulte la formule cherchée :

$$\sum_{d \in D_{n-1}} \zeta(d) = Card\,(\mathbf{Z}/n\mathbf{Z})^* = n-1 \; .$$

Question II.B.2.a

Soit H l'ensemble $\{\dot{1}, \dot{a}, \ldots, \dot{a}^{d-1}\}$. D'après la démonstration effectuée en II.A.4.a, H est de cardinal d. De plus pour tout j entier naturel, on a

$$\left(\dot{a}^j\right)^d - \dot{1} = \dot{a}^{dj} - \dot{1} = \dot{1} - \dot{1} = \dot{0}$$

puisque d divise dj et d'après la remarque faite en II.A.4.a.

En particulier tout élément de H est « racine du polynôme $X^d - \dot{1}$ ». Comme H est de cardinal d, II.A.3.a entraîne que $X^d - \dot{1}$ ne peut avoir de racines en dehors de H et donc l'ensemble des racines de $X^d - \dot{1}$ est, dans $\mathbf{Z}/n\mathbf{Z}$, $\{\dot{1}, \dot{a}, \ldots, \dot{a}^{d-1}\}$.

Question II.B.2.b

Soit k un entier naturel inférieur à d et m le pgcd de k et d. On peut écrire $k = bm$ et $d = cm$ pour des entiers naturels b et c. Si m est strictement plus grand que 1, c est donc un entier naturel non nul strictement inférieur à d et il vient

$$\left(\dot{a}^k\right)^c = \dot{a}^{bcm} = \dot{a}^{bd} = \dot{1} \; .$$

Par conséquent $\dot{a}^k$ est d'ordre inférieur à c, et donc d'ordre strictement inférieur à d.

Question II.B.2.c

Si $d = 1$, seul 1 est d'ordre 1 et on a $\zeta(1) = 1 = \varphi(1)$.

Soit maintenant d un diviseur de $n-1$ distinct de 1. S'il n'existe aucun élément d'ordre d, on a $\zeta(d) = 0$ et donc $\zeta(d) \leq \varphi(d)$.

Sinon, soit $\dot{a}$ un élément d'ordre d. D'après II.B.2.a les éléments d'ordre d s'écrivent nécessairement $\dot{a}^k$ pour k entier compris entre 0 et $d-1$, et même premiers avec d d'après II.B.2.b. Comme 0 n'est pas premier à d, puisque d est distinct de 1, un tel k appartient à S_d. Autrement dit seuls les éléments de la forme $\dot{a}^k$, pour k dans S_d sont susceptibles d'être d'ordre d. Il en résulte $\zeta(d) \leq \varphi(d)$.

Ainsi, dans tous les cas, on a $\zeta(d) \leq \varphi(d)$.

Il vient, d'après II.B.1 et I.5.e,

$$n-1 = \sum_{d \in D_{n-1}} \zeta(d) \leq \sum_{d \in D_{n-1}} \varphi(d) = n-1$$

et donc toutes les inégalités sont en fait des égalités : pour tout diviseur d de $n-1$, on a $\zeta(d) = \varphi(d)$.

En particulier $\zeta(n-1) = \varphi(n-1)$. D'après (E) ou encore puisque 1 appartient à S_{n-1} ou encore parce le cardinal d'un groupe est toujours strictement positif, $\varphi(n-1)$ est un entier naturel non nul. Il en résulte $\zeta(n-1) > 0$. Soit donc $\dot{b}$ un élément de $(\mathbf{Z}/n\mathbf{Z})^*$ d'ordre $n-1$. D'après II.B.2.a les racines, toutes distinctes, de $X^{n-1} - \dot{1}$, dans $(\mathbf{Z}/n\mathbf{Z})^*$, sont $\dot{1}$, $\dot{b}$, ..., $\dot{b}^{n-2}$. Ces $n-1$ éléments sont donc tous distincts et comme $(\mathbf{Z}/n\mathbf{Z})^*$ est de cardinal $n-1$, ce sont exactement ses éléments :

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

Question II.C.1

On a, d'après II.A.1,

$$(b+p)^{p-1} - b^{p-1} = p \sum_{k=0}^{p-1} (b+p)^k b^{p-1-k}$$

et donc

$$(b+p)^{p-1} - b^{p-1} = 0 \ mod\ p^2 \Leftrightarrow \sum_{k=0}^{p-2} (b+p)^k b^{p-2-k} = 0 \ mod\ p .$$

Or $b + p = b \ mod\ p$ et donc

$$(b+p)^{p-1} - b^{p-1} = 0 \ mod\ p^2 \Leftrightarrow \sum_{k=0}^{p-2} b^k b^{p-2-k} = 0 \ mod\ p \Leftrightarrow (p-1)b^{p-2} = 0 \ mod\ p .$$

Comme $\mathbf{Z}/p\mathbf{Z}$ est intègre et comme $p - 1 = -1 \ mod\ p$, il vient

$$(b+p)^{p-1} - b^{p-1} = 0 \ mod\ p^2 \Leftrightarrow b = 0 \ mod\ p .$$

Par conséquent $(b+p)^{p-1}$ et b^{p-1} ne peuvent être congrus modulo p^2 et donc l'un au moins n'est pas congru à 1 modulo p^2.

Question II.C.2

Pour r entier naturel, soit (H_r) la propriété : il existe un entier relatif k_r, premier avec p, tel que $c^{p^r(p-1)}$ soit égal à $1 + k_r p^{r+1}$.

Comme c est congru à b modulo p, c^{p-1} est congru à b^{p-1} modulo p et donc à 1. Il existe ainsi k_0 entier relatif tel que c^{p-1} soit égal à $1 + k_0 p$. De plus $c^{p-1} - 1$ est nul modulo p^2 si et seulement si k_0 est nul modulo p. Comme c a été choisi tel que c^{p-1} ne soit pas congru à 1 modulo p^2, k_0 n'est pas nul modulo p, i.e. k_0 est premier avec p.

Par conséquent (H_0) est vraie.

Maintenant, soit r un entier naturel et k_r un entier relatif premier à p tel que $c^{p^r(p-1)}$ soit égal à $1 + k_r p^{r+1}$. On a donc

$$c^{p^{r+1}(p-1)} = (1 + k_r p^{r+1})^p = 1 + k_r p^{r+2} + \sum_{j=2}^{p} \left(\begin{array}{c} p \\ j \end{array} \right) k_r^j p^{j(r+1)} .$$

Soit

$$k_{r+1} = k_r + \sum_{j=2}^{p} \left(\begin{array}{c} p \\ j \end{array} \right) k_r^j p^{(j-1)(r+1)-1} .$$

Pour j et r entier naturels avec $j \geq 2$, on a $(j-1)(r+1) \geq 1$ et $(j-1)(r+1) = 1$ si et seulement si $j = 2$ et $r = 0$.

Par conséquent, si $r > 0$, alors $k_{r+1} = k_r \ mod\ p$ et, si $r = 0$, alors $k_{r+1} = k_r(1 + p(p-1)k_r/2) \ mod\ p$.

Si p est impair, alors on a $k_{r+1} = k_r \ mod\ p$ dans tous les cas et donc k_{r+1} est premier à p, ce qui montre que (H_r) est héréditaire. Et donc le principe de récurrence permet d'affirmer que, pour tout entier naturel r, il existe un entier k_r, premier avec p, tel que $c^{p^r(p-1)}$ soit égal à $1 + k_r p^{r+1}$.

Remarque : **Si $p = 2$ le résultat est FAUX.** En effet dans ce cas b est n'importe quel entier impair et c est un entier congru à 3 modulo 4. Si $c = 4k - 1$ avec k entier naturel non nul, on a $c = 1 + (2k-1) \times 2$ et $c^2 = 1 + 8k(2k-1)$ et donc c^2 ne peut pas s'écrire $1 + 4k_1$ avec k_1 premier à 2. Pour la suite on se placera donc dans le cas p impair.

Question II.C.3.a

Comme $(\mathbf{Z}/n\mathbf{Z})^*$ est d'ordre $\varphi(n)$, il est d'ordre $p^{\alpha-1}(p-1)$, d'après la formule (E). D'après II.A.4.a l'ordre de $\dot{c}$ divise le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$ et donc r divise $p^{\alpha-1}(p-1)$.

Puisque c^r est congru à 1 modulo n, en particulier il est congru à 1 modulo p. Or c est congru à b modulo p et est donc d'ordre $p-1$ modulo p. Soit q et a les quotient et reste de la division euclidienne de r par $p-1$, on a

$$c^r = (c^{p-1})^q c^a = 1^q c^a = c^a \ mod\ p$$

et donc, puisque a est inférieur à l'ordre de $\dot{c}$ dans $(\mathbf{Z}/p\mathbf{Z})^*$, a doit être nul, i.e. $p-1$ doit diviser r, ce qui est l'assertion recherchée.

Question II.C.3.b

Puisque $p-1$ divise r, il existe un entier naturel non nul k tel que $r = (p-1)k$. Soit k un tel entier ; r divise $(p-1)p^{\alpha-1}$ si et seulement si k divise $p^{\alpha-1}$ et donc si et seulement si k peut s'écrire p^β avec β entier naturel inférieur à $\alpha - 1$.

Par conséquent il existe β un entier naturel inférieur à $\alpha - 1$ tel que $r = p^\beta(p-1)$.

Question II.C.3.c

Soit donc β un entier naturel inférieur à $\alpha - 1$ tel que $r = p^\beta(p-1)$. D'après II.C.2, on peut trouver un entier k_β premier à p tel que $c^r = 1 + k_\beta p^{\beta+1}$. En particulier, puisque c^r est congru à 1 modulo p^α, $k_\beta p^{\beta+1}$ est divisible par p^α. Comme k_β est premier à p, ceci impose $\alpha \leq \beta + 1$ et donc, puisque $\beta \leq \alpha - 1$, on a $\beta = \alpha - 1$.

L'ordre de $\dot{c}$ dans $(\mathbf{Z}/n\mathbf{Z})^*$ est donc égal à l'ordre de ce groupe. Comme il a été remarqué en II.4.a et en II.B.2.c ceci entraîne que $(\mathbf{Z}/n\mathbf{Z})^*$ est égal à $\{1, \dot{c}, \ldots, \dot{c}^{r-1}\}$, i.e. $\dot{c}$ est un générateur de $(\mathbf{Z}/n\mathbf{Z})^*$.

Question II.C.4

Le groupe $(\mathbf{Z}/7\mathbf{Z})^*$ est de cardinal 6. On cherche donc des éléments d'ordre 6. Les ordres des éléments de $(\mathbf{Z}/7\mathbf{Z})^*$ sont respectivement 1, 3, 6, 3, 6, 2 pour $\dot{1}$, $\dot{2}$, $\dot{3}$, $\dot{4}$, $\dot{5}$ et $\dot{6}$.

Par conséquent $\dot{3}$ est un générateur de $(\mathbf{Z}/7\mathbf{Z})^*$.

Le groupe $(\mathbf{Z}/49\mathbf{Z})^*$ est de cardinal $\varphi(49)$, soit 7×6, i.e. 42. D'après ce qui précède parmi $\dot{3}$ et $\dot{3} + \dot{7}$, l'un des deux a sa puissance sixième qui n'est pas congru à 1 modulo 49 et alors celui-là est d'ordre 42. Comme $\dot{10}$ est de carré $\dot{2}$, sa puissance sixième est $\dot{8}$, ce qui n'est pas $\dot{1}$. Par conséquent $\dot{10}$ est un générateur de $(\mathbf{Z}/49\mathbf{Z})^*$.

Remarque : En fait $\dot{3}$, $\dot{5}$, $\dot{10}$ et $\dot{12}$ sont tous les quatre des générateurs de $(\mathbf{Z}/49\mathbf{Z})^*$.

Partie III

Question III.1.a

Puisque p est impair, $(p-1)/2$ est un entier. La question II.A.4.b montre

$$(a^{(p-1)/2})^2 \equiv 1 \; mod \; p$$

et la question II.A.3.a montre que le polynôme $X^2 - \dot{1}$ n'a que deux racines au plus dans $\mathbf{Z}/p\mathbf{Z}$. Or $\dot{1}$ et $-\dot{1}$ sont tous les deux des racines de ce polynôme. Comme p n'est pas 2, ces deux racines sont distinctes et ce sont donc les seules. Il en résulte que $a^{(p-1)/2}$ est congru soit à 1, soit à -1 modulo p, ou encore

$$a^{(p-1)/2} \equiv 1 \; mod \; p \qquad \text{ou} \qquad a^{(p-1)/2} \equiv p-1 \; mod \; p \; .$$

Question III.1.b

Soit a un entier naturel premier à p. Notons E l'ensemble des entiers naturels r tels que $a^{q\times 2^r}$ soit congru à 1 modulo p. D'après II.4.b E contient s et est donc non vide. Toute partie non vide de $\mathbf{N}$ ayant un plus petit élément, on peut condiérer k le plus petit élement de E. Si k est nul, alors on a $a^q \equiv 1 \; mod \; p$ et donc a vérifie $H_a(p)$.

Si maintenant k n'est pas nul, notons $r = k-1$ et $b = a^{q\times 2^r}$. Alors b n'est pas congru à 1 modulo p, par définition de k, mais b^2 l'est. Par conséquent, comme en III.1.a, b est congru à $p-1$ modulo p et il en résulte que a vérifie $H_a(p)$.

Question III.2

Soit a un entier tel que p soit a-ppf. S'il existe un entier r compris entre 0 et $s-1$ tel que $a^{q\times 2^r} \equiv p-1 \; mod \; p$, alors $a^{q\times 2^{r+1}} \equiv 1 \; mod \; p$ et donc, si p est a-ppf il existe un entier n de la forme $q \times 2^r$ avec $0 \leq r \leq s$ tel que a^n soit congru à 1 modulo p. En particulier a est inversible modulo p et donc, d'après les rappels en début de partie II, a est premier avec p.

Par contraposée, si a est un entier dont le PGCD avec p est strictement plus grand que 1, il n'est pas premier avec p et donc p n'est pas a-ppf.

Question III.3.a

Voici le programme en langage TI-89. On initialise q à $p-1$ et s à 0, puis on divise successivement q par 2, tant qu'il est pair, et on incrémente s de 1. Au final on a des valeurs q et s telles que $p-1 = q \times 2^s$ avec q impair. Ensuite on initialise b à 1 et on prend q fois de suite le reste de la division euclidienne de ab par p. Au final on obtient donc dans b le reste de la division euclidienne de a^q par p. Si b vaut 1, p est a-ppf grâce à la première propriété et on affiche « $a^q = 1$ ». Sinon on initialise r à 0 et tant qu'il est inférieur strictement à s, on teste si b vaut $p-1$. Si oui, p est a-ppf pour la seconde propriété et on affiche « $a^{q\times 2^r} = 1$ ». Si non, on incrémente r et on change b en (le reste de la division euclidienne par p de) son carré. Si on n'a trouvé aucun r, alors p n'est pas a-ppf et on affiche cela.

```
ppf(a,p)
Prgm
p-1 -> q
0 -> s
While mod(q,2)=0
q/2 -> q
s+1 -> s
EndWhile
1 -> b
For i,1,q
mod(a*b,p) -> b
EndFor
If b=1 Then
Disp "a^q=1"
```

```
Else
0 -> r
While r<s
If b=p-1 Then
Disp "a^(q*2^r)=p-1"
Exit
EndIf
r+1 -> r
mod(b^2,p) -> b
EndWhile
If r=s Then
Disp "p n'est pas a-ppf"
EndIf
EndIf
EndPrgm
```

Question III.3.b

p	49	91	111	121	135	1225
a	30	74	28	94	43	999
p est a-ppf	Oui	Oui	Non	Oui	Non	Oui
Relation	$a^3 = 1$	$a^{45} = 1$		$a^{15} = 120$		$a^{153} = 1224$

Question III.3.c

Grâce au programme, en langage TI-89,

```
ppf561(a)
Prgm
a -> b
For i,1,10
Pause b
mod(a*b,561) -> b
EndFor
EndPrgm
```

On constate, grâce à ppf561(50), que $\dot{50}$ admet comme puissances successives, de 1 à 10, les classes de 50, 256, 458, 460, 560, 511, 305, 103, 101 et 1 modulo 561. Et donc l'ensemble des classes modulo 561 des entiers a tels que 561 soit a-ppf est exactement le groupe cyclique, d'ordre 10, engendré par $\dot{50}$.

Partie IV

Question IV.A.1

Supposons que n s'écrit $n = p_1 \times p_2 \times \ldots \times p_k$ pour k un entier naturel supérieur à 2 et p_1, p_2, ..., p_k des nombres premiers deux à deux distincts tels que $p_i - 1$ divise $n - 1$ pour tout entier naturel non nul i inférieur à k. En particulier n n'est pas premier.

Soit a un nombre premier avec n et i un entier naturel non nul inférieur à k. Comme a est premier à n, il est également premier à p_i et donc, d'après II.A.4.b, a^{p_i-1} est congru à 1 modulo p_i. Mais comme $p_i - 1$ divise $n - 1$, d'après la remarque faite en II.A.4.a a^{n-1} est également congru à 1 modulo p_i.

Autrement dit p_i divise $a^{n-1}-1$ pour tout entier naturel i inférieur à k, donc $a^{n-1}-1$ est divisible par le PPCM de $(p_i)_{1\leq i\leq k}$, c'est-à-dire n, puisque les $(p_i)_{1\leq i\leq k}$ sont premiers entre eux.

En conclusion si a est un nombre premier à n, a^{n-1} est congru à 1 modulo n et donc n est un nombre de Carmichaël.

Question IV.A.2.a

On a $\varphi(2^\alpha)=2^{\alpha-1}(2-1)=2^{\alpha-1}$ et donc $(\mathbf{Z}/n\mathbf{Z})^*$ est de cardinal $n/2$.

Si a est un entier impair, il est premier avec 2 et donc avec n. Il est donc inversible modulo n et donc $a^{n/2}$ est congru à 1 modulo n, d'après II.A.4.a. A fortiori a^n l'est également, de sorte que a^{n-1} est congru à a^{-1} modulo n. Par conséquent, $a^{2^\alpha-1}$ ne peut être congru à 1 modulo n que si a l'est.

Comme $(\mathbf{Z}/n\mathbf{Z})^*$ est de cardinal $n/2$, il ne comporte un seul élément que si $n=2$ et donc, si $n=2^\alpha$ avec α un entier supérieur à 2, n n'est pas un nombre de Carmichaël. Ou encore : tout nombre de Carmichaël possède au moins un facteur premier impair.

Question IV.A.2.b.I

D'après I.4, S_n est en bijection avec $S_{p_1^{\alpha_1}}\times S_{p_2^{\alpha_2}\dots p_k^{\alpha_k}}$ par l'application qui à un élément t associe les restes de ses divisions euclidiennes par $p_1^{\alpha_1}$ et $p_2^{\alpha_2}\dots p_k^{\alpha_k}$, puisque ces deux nombres sont premiers entre eux.

Soit donc a le reste de la division euclidienne de ω par $p_1^{\alpha_1}$. La classe de a et celle de ω sont les mêmes modulo $p_1^{\alpha_1}$ et a est donc premier avec $p_1^{\alpha_1}$. C'est donc un élément de $S_{p_1^{\alpha_1}}$. Comme 1 est premier avec n'importe qui, il appartient à $S_{p_2^{\alpha_2}\dots p_k^{\alpha_k}}$. Soit donc t l'antécédent de $(a,1)$ par la bijection précitée. On a

$$t\equiv a\equiv\omega\ mod\ p_1^{\alpha_1}\qquad\qquad t\equiv 1\ mod\ p_2^{\alpha_2}\dots p_k^{\alpha_k}$$

et donc

$$t\equiv a\equiv\omega\ mod\ p_1^{\alpha_1}\qquad\qquad \forall i\in 2,\dots,k\quad t\equiv 1\ mod\ p_i\ .$$

Par construction de la bijection t appartient à S_n et est donc premier à n. Comme n est un nombre de Carmichaël, on a donc $t^{n-1}\equiv 1\ mod\ n$.

Question IV.A.2.b.II

Soit r un entier naturel non nul et x la réduction modulo n de t^r. Puisque t est premier à n, il en est de même de t^r, donc de x. Par conséquent, comme h construite en I.4 est une bijection, x est égal à 1 si et seulement si $h(x)=h(1)=(1,1)$. Or, en notant, $h(x)=(a,b)$, on a

$$a\equiv x\equiv t^r\equiv\omega^r\ mod\ p_1^{\alpha_1}\qquad\text{et}\qquad b=1\ .$$

Par conséquent $x=1$ si et seulement si r est un multiple de l'ordre de la classe de ω dans $(\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^*$, i.e. $\varphi(p_1^{\alpha_1})$, ou encore $p_1^{\alpha_1-1}(p_1-1)$, puisque la classe de ω est un générateur de $(\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^*$.

En résumé t^r est congru à 1 modulo n si et seulement si r est un multiple de $p_1^{\alpha_1-1}(p_1-1)$. Par conséquent, d'après ce qui précède, $p_1^{\alpha_1-1}(p_1-1)$ divise $n-1$.

Comme n et $n-1$ vérifient la relation de Bézout $n-(n-1)=1$, ils sont premiers entre eux et en particulier p_1 est premier avec $n-1$. Comme $p_1^{\alpha_1-1}$ divise $n-1$, c'est que α_1-1 est nul, i.e. $\alpha_1=1$.

Autrement dit $p_1^{\alpha_1-1}(p_1-1)=p_1-1$ et donc, d'après ce qui précède p_1-1 divise $n-1$.

Question IV.A.2.b.III

Comme p_1 est impair, p_1-1 est pair et donc $n-1$ aussi, puisque p_1-1 divise $n-1$. Il en résulte que n est impair et ne possède donc que des facteurs premiers impairs. La question précédente montre que tous les facteurs premiers de n apparaissent avec un exposant 1 dans la décomposition de n et que si p est l'un d'eux, alors $p-1$ divise $n-1$.

D'où la conclusion : un nombre n est un nombre de Carmichaël si et seulement si n s'écrit $n=p_1\times p_2\times\ldots\times p_k$ pour k un entier naturel supérieur à 2 et p_1, p_2, …, p_k des nombres premiers impairs deux à deux distincts tels que p_i-1 divise $n-1$ pour tout entier naturel non nul i inférieur à k.

Question IV.A.3

Soit p et q deux nombres premiers impairs distincts, avec $p < q$. On a

$$p(q-1) = pq - p < pq - 1 < pq - 1 + q - p = (p+1)(q-1)$$

et donc $q-1$ ne divise pas $pq-1$. Par conséquent pq ne peut être un nombre de Carmichaël et, ainsi, un nombre de Carmichaël possède au moins trois facteurs premiers.

Question IV.A.4

On a la relation de Bézout $16 \times 16 - 3 \times 85 = 1$ et donc les solutions de $85p - 16k = 1$ avec k et p entiers sont les couples $(k,p) = (-16 + 85m, -3 + 16m)$ avec m entier relatif.

En effet, si k et p sont deux entiers relatifs, on a

$$85p - 16k - 1 = 85(p+3) - 16(k+16)$$

et donc, si $85p - 16k = 1$, alors, puisque 85 et 16 sont premiers entre eux, 16 divise $p+3$ et 85 divise $k+16$, et l'assertion en découle.

Soit maintenant p un nombre premier impair distinct de 5 et 17 et $n = 5 \times 17 \times p$. D'après IV.A.2, n est un nombre de Carmichaël si et seulement si 4, 16 et $p-1$ divisent $n-1$, i.e. si et seulement si 16 et $p-1$ divisent $85p-1$. Pour que 16 divise $85p-1$, il faut et il suffit qu'il existe un entier relatif k tel que $85p - 1 = 16k$ et donc p est congru à -3 modulo 16. La plus petite valeur de p possible est donc 13. C'est un nombre premier et de plus $13-1$ vaut 12 et divise $85 \times 13 - 1$ qui vaut 1104.

Par conséquent le plus petit nombre de Carmichaël divisible par 5 et 17 est 1105.

Question IV.B.1

Remarque : On ne s'intéresse qu'au cas où n est impair, sinon la définition de a-ppf n'existe pas.

Soit a un entier naturel premier à n. Comme n n'est ni premier, ni un nombre de Carmichaël, il possède un facteur premier impair avec un exposant strictement supérieur à 1. Autrement dit il existe un nombre premier impair p_1 et un entier naturel α_1 supérieur à 2 tels que $p_1^{\alpha_1}$ divise n

Écrivons $n - 1 = q \times 2^s$ avec q impair et s entier naturel. On a déjà remarqué en III.2 que si n est a-ppf, alors il existe un entier naturel r inférieur à s tel que $a^{q \times 2^r}$ soit congru à 1 modulo p. D'après la remarque faite en II.A.4.a, ceci entraîne que l'ordre de la classe de a divise $q \times 2^r$ et donc divise $n-1$.

Soit t l'élément construit en IV.2.b.I, on a montré que l'ordre de sa classe modulo n est $p_1^{\alpha_1 - 1}(p_1 - 1)$. Comme n et $n-1$ sont premiers entre eux, p_1 est premier à $n-1$ et donc $p_1^{\alpha_1 - 1}(p_1 - 1)$ ne divise pas $n-1$. En particulier n n'est pas t-ppf.

Par conséquent, si n est un nombre impair non premier et qui n'est pas un nombre de Carmichaël, il existe au moins un entier inférieur à n et premier avec n tel que n ne soit pas a-ppf.

Remarque : Un nombre non premier et qui n'est pas un nombre de Carmichaël est tout simplement un nombre divisible par le carré d'un nombre premier.

Question IV.B.2

Soit n un nombre impair composé.

Puisque l'ensemble des classes d'entiers naturels a strictement inférieurs à n tels que n soit a-ppf est inclus dans un certain sous-groupe H strict de $(\mathbf{Z}/n\mathbf{Z})^*$, le nombre de telles classes est inférieur au cardinal de H. Or ce cardinal est un diviseur de celui de $(\mathbf{Z}/n\mathbf{Z})^*$ et même un diviseur strict, puis H est un sous-groupe strict. Autrement dit le cardinal H est un diviseur strict de $\varphi(n)$ et donc est inférieur à $\varphi(n)/2$.

Par conséquent la probabilité de tirer un nombre entier naturel non nul a, inférieur strictement à n et tel que n soit a-ppf, est inférieure à $\varphi(n)/2n$ et donc à $1/2$.

Il en résulte que la probabilité de déclarer n premier est inférieure à $1/2^k$.