

Correction de l'épreuve d'algèbre  
Capes 2003

Calixte Denizet  
calixteman@yahoo.fr

18 avril 2003

# Partie I

I.1.a. On a trivialement

$$A_2 = (A_2 \cap A_1) \cup (A_2 \cap \overline{A_1}) \text{ et } (A_2 \cap A_1) \cap (A_2 \cap \overline{A_1}) = \emptyset$$

On en déduit donc que

$$\begin{aligned} P(A_2) &= P(A_2 \cap A_1) + P(A_2 \cap \overline{A_1}) \iff P(A_2 \cap \overline{A_1}) = P(A_2) - P(A_2 \cap A_1) \\ &\iff P(A_2 \cap \overline{A_1}) = P(A_2)(1 - P(A_1)) \\ &\iff P(A_2 \cap \overline{A_1}) = P(A_2)P(\overline{A_1}) \end{aligned}$$

On peut conclure que les évènements  $A_2$  et  $\overline{A_1}$  sont indépendants.

I.1.b.(i). Dire que les évènements  $A_1, A_2, \dots, A_k$  sont mutuellement indépendants est équivalent à dire que pour toute sous-famille  $A_{i_1}, \dots, A_{i_n}$  d'évènements distincts on a

$$P(A_{i_1} \cap \dots \cap A_{i_n}) = P(A_{i_1}) \dots P(A_{i_n})$$

Soit donc  $A_{i_1}, \dots, A_{i_n}$  une sous-famille de  $A_2, \dots, A_k$ , on a compte tenu de la question précédente et du fait que les évènements  $A_1$  et  $A_{i_1} \cap \dots \cap A_{i_n}$  sont indépendants

$$\begin{aligned} P(\overline{A_1} \cap (A_{i_1} \cap \dots \cap A_{i_n})) &= P(A_{i_1} \cap \dots \cap A_{i_n}) P(\overline{A_1}) \\ &= P(A_{i_1}) \dots P(A_{i_n}) P(\overline{A_1}) \end{aligned}$$

Ainsi les évènements  $\overline{A_1}, A_2, \dots, A_k$  sont indépendants.

I.1.b.(ii). Nous allons montrer par récurrence sur  $1 \leq n \leq k$  que les évènements  $\overline{A_1}, \dots, \overline{A_n}, A_{n+1}, \dots, A_k$  sont indépendants.

- amorce :  $n = 1$  : cela a été fait à la question précédente.
- hérédité : on suppose la propriété vraie au rang  $n - 1$ . Alors la question précédente permet encore de conclure que  $\overline{A_1}, \dots, \overline{A_n}, A_{n+1}, \dots, A_k$  sont indépendants.

I.2.a. Il existe 50 multiples de 2 compris entre 1 et 100 donc

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

Il existe 20 multiples de 5 compris entre 1 et 100 donc

$$P(A_2) = \frac{20}{100} = \frac{1}{5}$$

L'évènement  $A_1 \cap A_2$  est équivalent à l'évènement " $X$  multiple de 10". Or il existe 10 multiples de 10 compris entre 1 et 100 donc

$$P(A_1 \cap A_2) = \frac{10}{100} = \frac{1}{10} = \frac{1}{2} \times \frac{1}{5} = P(A_1)P(A_2)$$

On en conclut que  $A_1$  et  $A_2$  sont indépendants.

I.2.b. En procédant de même qu'à la question précédente, on a

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

Puisque  $\frac{20}{101} \times \frac{50}{101} \neq \frac{10}{101}$ , les évènements ne sont alors pas indépendants.

I.3.a. On a

$$P(A) = \frac{\text{Card} \{x \wedge n = 1 \mid x \in \llbracket 1; n \rrbracket\}}{\text{Card } \Omega} = \frac{\phi(n)}{n}$$

I.3.b. On a

$$P(A_i) = \frac{\text{Card} \{x \text{ multiple de } p_i, x \in \llbracket 1; n \rrbracket\}}{\text{Card } \Omega}$$

et

$$x \text{ multiple de } p_i \iff \exists k \in \mathbb{N}^* \quad x = kp_i$$

Puisque  $x \in \llbracket 1; n \rrbracket$ , on a  $k \leq \frac{n}{p_i} \in \mathbb{N}$  et on en déduit que

$$P(A_i) = \frac{\text{Card} \llbracket 1; \frac{n}{p_i} \rrbracket}{\text{Card } \Omega} = \frac{\frac{n}{p_i}}{n} = \frac{1}{p_i}$$

I.3.c. Soit  $(A_{i_1}, \dots, A_{i_j})$  une sous-famille de  $(A_i)_{1 \leq i \leq k}$ . L'évènement  $A_{i_1} \cap \dots \cap A_{i_j}$  est équivalent à l'évènement " $X$  multiple de  $p_{i_1} \dots p_{i_j}$ ". Or

$$\begin{aligned} \text{Card} \{x \text{ multiple de } p_{i_1} \dots p_{i_j}, x \in \llbracket 1; n \rrbracket\} &= \text{Card} \llbracket 1; \frac{n}{p_{i_1} \dots p_{i_j}} \rrbracket \\ &= \frac{n}{p_{i_1} \dots p_{i_j}} \end{aligned}$$

On en déduit

$$P(A_{i_1} \cap \dots \cap A_{i_j}) = \frac{\frac{n}{p_{i_1} \dots p_{i_j}}}{n} = \frac{1}{p_{i_1} \dots p_{i_j}} = \frac{1}{p_{i_1}} \dots \frac{1}{p_{i_j}} = P(A_{i_1}) \dots P(A_{i_j})$$

Par conséquent, les évènements  $(A_i)_{1 \leq i \leq k}$  sont mutuellement indépendants.

I.3.d. On a

$$\begin{aligned} x \wedge n = 1 \text{ avec } n = \prod_{i=1}^k p_i^{\alpha_i} &\iff \forall i \in \llbracket 1; k \rrbracket \quad p_i \nmid x \\ &\iff \forall i \in \llbracket 1; k \rrbracket \quad x \text{ non multiple de } p_i \end{aligned}$$

On en déduit immédiatement que

$$A = \bigcap_{i=1}^k \overline{A_i}$$

I.3.e. Des questions I.1.b.(ii) et I.3.c., on déduit que les  $(\overline{A_i})_{1 \leq i \leq k}$  sont indépendants. Donc

d'après les questions I.3.a., I.3.b. et I.3.d., on a

$$\begin{aligned}
P(A) &= \prod_{i=1}^k P(\overline{A_i}) \\
&= \prod_{i=1}^k (1 - P(A_i)) \\
&= \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) \\
&= \frac{\phi(n)}{n}
\end{aligned}$$

On en conclut que

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

I.4.a. Soit  $\tau \in S_{pq}$  et  $(a, b) = h(\tau) \in \llbracket 0; p-1 \rrbracket \times \llbracket 0; q-1 \rrbracket$ . Montrons que  $a \in S_p$ .

On a, par division euclidienne,

$$\tau = \alpha p + a$$

Ainsi  $a \wedge p | \tau$ , or  $a \wedge p | p$  donc  $a \wedge p | \tau \wedge p$ . Mais  $\tau \wedge p$  divisant  $\tau \wedge pq = 1$ , on en déduit que  $a \wedge p | 1$  donc  $a \wedge p = 1$ . On en conclut que  $a \in S_p$ . De même, on a  $b \in S_q$ .

Ainsi  $(a, b) \in S_p \times S_q$ , d'où  $h(S_{pq}) \subset S_p \times S_q$ .

I.4.b. Soient  $(\tau, \tau') \in S_{pq}$  tels que  $h(\tau) = h(\tau')$ . On a

$$\begin{cases} \tau \equiv \tau' & [p] \\ \tau \equiv \tau' & [q] \end{cases}$$

Donc  $p | (\tau - \tau')$  et  $q | (\tau - \tau')$ . Or  $p \wedge q = 1$  donc  $pq | (\tau - \tau')$  d'où il existe  $k \in \mathbb{N}$  tel que  $\tau = \tau' + kpq \leq pq$  ce qui implique que  $k = 0$  donc que  $\tau = \tau'$ .

Par conséquent,  $h$  est injective.

I.4.c. L'existence de  $(\alpha, \beta) \in \mathbb{Z}^2$  découle directement du fait que  $p \wedge q = 1$  et du théorème de Bézout.

De la relation  $\alpha p + \beta q = 1$  on déduit

$$\begin{cases} \beta q \equiv 1 & [p] \\ \alpha p \equiv 1 & [q] \end{cases}$$

Et on obtient

$$\begin{cases} x \equiv \beta q a \equiv 1 a \equiv a & [p] \\ x \equiv \alpha p b \equiv 1 b \equiv b & [q] \end{cases}$$

Montrons maintenant que  $x$  ainsi défini est dans  $S_{pq}$  c'est à dire que  $x \wedge pq = 1$ .

On a  $x \equiv a [p]$  donc il existe  $k \in \mathbb{N}$  tel que  $x = kp + a$ , ainsi  $x \wedge p | a$ . Or  $x \wedge p | p$  donc  $x \wedge p | a \wedge p = 1$  d'où  $x \wedge p = 1$ . De même on a  $x \wedge q = 1$ . On en conclut que  $x \wedge pq = 1$  donc  $x \in S_{pq}$  puis que  $S_p \times S_q \subset h(S_{pq})$ . De la question I.4.a., on peut conclure que  $S_p \times S_q = h(S_{pq})$  donc que  $h$  est surjective puis que  $h$  est bijective.

De la bijectivité de  $h$ , on a

$$\text{Card } S_{pq} = \text{Card } S_p \times \text{Card } S_q \iff \phi(pq) = \phi(p)\phi(q)$$

I.4.d. On procède par récurrence sur le nombre  $k$  de facteurs premiers de  $n$ .

– amorce :  $k = 1 : n = p^\alpha$  avec  $p$  premier et  $\alpha \geq 1$ .

Remarquons tout d'abord que  $x \wedge p^\alpha = 1$  est équivalent à  $x$  non multiple de  $p$ . On a

$$\text{Card } S_{p^\alpha} = \text{Card } \llbracket 1; p^\alpha \rrbracket - \text{Card } \llbracket 1; p^{\alpha-1} \rrbracket = p^\alpha \left( 1 - \frac{1}{p} \right)$$

Donc

$$\phi(p^\alpha) = p^\alpha \left( 1 - \frac{1}{p} \right)$$

– hérédité : supposons la propriété vraie au rang  $k - 1$ . Soit  $n = \prod_{i=1}^k p_i^{\alpha_i}$ . On a

$$\left( \prod_{i=1}^{k-1} p_i^{\alpha_i} \right) \wedge p_k^{\alpha_k} = 1 \text{ car les } p_k \text{ sont premiers}$$

D'après la question précédente, on a

$$\phi(n) = \phi \left( \prod_{i=1}^{k-1} p_i^{\alpha_i} \right) \phi(p_k^{\alpha_k})$$

D'après l'hypothèse de récurrence et l'amorce, on a

$$\begin{aligned} \phi(n) &= \prod_{i=1}^{k-1} p_i^{\alpha_i} \prod_{i=1}^{k-1} \left( 1 - \frac{1}{p_i} \right) p_k^{\alpha_k} \left( 1 - \frac{1}{p_k} \right) \\ &= n \prod_{i=1}^k \left( 1 - \frac{1}{p_i} \right) \end{aligned}$$

Ainsi la propriété est vérifiée au rang  $k$ .

I.5.a. Puisque  $a \wedge n | a$ , il existe alors  $k \in \mathbb{N}$  tel que  $a = kd$ . De  $k | a$ , on déduit que  $k \wedge \frac{n}{d} | a \wedge \frac{n}{d}$  et de  $\frac{n}{d} | n$ , on déduit que  $a \wedge \frac{n}{d} | a \wedge n$ . Puis de  $a \wedge n = 1$ , on peut conclure que  $k \wedge \frac{n}{d} = 1$ . Montrons maintenant la réciproque.

Supposons  $a = kd$  avec  $k \wedge \frac{n}{d} = 1$ . Puisque  $d | a$  et  $d | n$  alors  $d | a \wedge n$ . De plus le théorème de Bézout permet d'affirmer que

$$\begin{aligned} \exists(\alpha, \beta) \in \mathbb{Z}^2 \quad \alpha k + \beta \frac{n}{d} = 1 &\iff \alpha kd + \beta n = d \\ &\iff \alpha a + \beta n = d \end{aligned}$$

Or  $a \wedge n | a$  et  $a \wedge n | n$  donc d'après la relation précédente on a  $a \wedge n | d$ . On en conclut que  $a \wedge n = d$ . De l'équivalence venant d'être établie, on peut déduire que

$$\{a \in \llbracket 1; n \rrbracket \mid a \wedge n = d\} \text{ est en bijection avec } \left\{ k \in \llbracket 1; n \rrbracket \mid k \wedge \frac{n}{d} = 1 \right\} = S_{\frac{n}{d}}$$

Donc

$$\text{Card } \{a \in \llbracket 1; n \rrbracket \mid a \wedge n = d\} = \phi \left( \frac{n}{d} \right)$$

I.5.b. On a clairement

$$P(C_d) = \frac{\text{Card} \{a \in \llbracket 1; n \rrbracket \mid a \wedge n = d\}}{\text{Card } \Omega} = \frac{1}{n} \phi\left(\frac{n}{d}\right)$$

I.5.c. La famille d'évènements  $(C_d)_{d \in D_n}$  forme une partition de  $\Omega$ . En effet, les  $(C_d)_{d \in D_n}$  sont clairement non vides, deux à deux disjoints et on a

$$\bigcup_{d \in D_n} C_d = \{a \in \llbracket 1; n \rrbracket \mid \exists d \in \llbracket 1; n \rrbracket \quad a \wedge n = d\} = \llbracket 1; n \rrbracket$$

On en déduit que

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

I.5.d. Si  $d$  est un diviseur de  $n$  alors  $\frac{n}{d}$  est un diviseur de  $n$ . Le fait que  $u$  soit bijective s'en déduit trivialement. On peut donc effectuer le changement de variable  $d' = u(d)$  dans la somme précédente et l'on obtient

$$\sum_{d' \in D_n} \frac{1}{n} \phi(d') = 1 \iff \sum_{d \in D_n} \phi(d) = n$$

## Partie II

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

II.A.1. On a

$$\begin{aligned} (b-a) \sum_{k=0}^{n-1} b^{n-1-k} a^k &= \sum_{k=0}^{n-1} b^{n-k} a^k - \sum_{k=0}^{n-1} b^{n-(k+1)} a^{k+1} \\ &= \sum_{k=0}^{n-1} b^{n-k} a^k - \sum_{\ell=1}^n b^{n-\ell} a^\ell \\ &= b^n + \sum_{k=1}^{n-1} b^{n-k} a^k - \sum_{\ell=1}^{n-1} b^{n-\ell} a^\ell - a^n \\ (b-a) \sum_{k=0}^{n-1} b^{n-1-k} a^k &= b^n - a^n \end{aligned}$$

Ainsi le quotient de  $b^n - a^n$  par  $b - a$  est

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

II.A.2. Supposons que  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  soit un corps. Soit  $x \in \llbracket 1; n-1 \rrbracket$ . Puisque  $\mathbb{Z}/n\mathbb{Z}$  est un corps, l'élément  $\dot{x} \neq \dot{0}$  est inversible donc il existe  $\dot{u} \in \mathbb{Z}/n\mathbb{Z}$  tel que  $\dot{u}\dot{x} = \dot{1}$ . Ainsi il existe  $k \in \mathbb{Z}$  tel que  $ux = 1 + kn$  soit  $ux - kn = 1$  ce qui implique que  $x \wedge n = 1$ . Nous

venons de montrer que pour tout  $x \in \llbracket 1; n-1 \rrbracket$ , nous avons  $x \wedge n = 1$  ce qui signifie que  $n$  est premier.

Réciproquement, supposons que  $n$  soit premier c'est à dire que pour tout  $x \in \llbracket 1; n-1 \rrbracket$  nous avons  $x \wedge n = 1$ . D'après le théorème de Bézout

$$\exists(\alpha, \beta) \in \mathbb{Z}^2 \quad \alpha x + \beta n = 1$$

Passant modulo  $n$ , nous obtenons

$$\alpha \dot{x} = \dot{1}$$

ce qui signifie que  $\dot{x}$  est inversible dans  $\mathbb{Z}/n\mathbb{Z}$ . Ceci étant vrai pour tout  $\dot{x} \neq \dot{0}$ , on en déduit que  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un corps.

II.A.3.a. Démontrons par récurrence sur le degré  $k$  de  $P \in (\mathbb{Z}/n\mathbb{Z})[X]$  que  $P$  admet au plus  $k$  racines.

– amorce :  $k=1$  :  $P$  est de la forme  $P(X) = \alpha X + \beta$  avec  $\alpha \neq \dot{0}$ . On a donc

$$P(X) = 0 \iff \alpha X + \beta = 0 \iff X = -\beta\alpha^{-1} \text{ (car } \mathbb{Z}/n\mathbb{Z} \text{ est un corps)}$$

$P$  admet donc au plus 1 racine.

– hérédité : supposons la propriété vraie au rang  $k-1$ . Soit un polynôme  $P$  de degré  $k$ . Si  $P$  n'admet aucune racine, alors la propriété est démontrée. Supposons alors que  $P$  admette au moins une racine  $\lambda$ , on a alors

$$\exists Q \in (\mathbb{Z}/n\mathbb{Z})[X] \quad P(X) = (X - \lambda)Q(X) \text{ avec } \deg Q = k-1$$

On peut appliquer l'hypothèse de récurrence à  $Q$ , pour en déduire qu'il admet au plus  $k-1$  racines. On en conclut que  $P$  admet au plus  $k$  racines. La propriété est donc vraie au rang  $k$ .

II.A.3.b. On a  $P(\dot{0}) = \dot{0}$ ,  $P(\dot{1}) = \dot{0}$ ,  $P(\dot{2}) = \dot{2}$ ,  $P(\dot{3}) = \dot{0}$ ,  $P(\dot{4}) = \dot{0}$  et  $P(\dot{5}) = \dot{2}$ . Donc  $P$  qui est de degré 2 admet quatre racines. On en conclut que, dans la question précédente, la condition  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  est un corps est nécessaire.

II.A.3.c. On a comme factorisations possibles  $P(X) = X(X-1)$  et  $P(X) = (X-3)(X-4)$ .

II.A.4.a. Montrons que  $H = \{1, x, \dots, x^{k-1}\}$  est un sous-groupe de  $G$ . Clairement  $H \subset G$  et

– on a  $1 \in H$ .

– soient  $(a, b) \in H^2$ . Il existe alors  $(\alpha, \beta) \in \llbracket 0; k-1 \rrbracket^2$  tel que  $a = x^\alpha$  et  $b = x^\beta$ . On a alors  $ab^{-1} = x^{\alpha-\beta}$ . On effectue la division euclidienne de  $\alpha - \beta$  par  $k$ , il existe alors  $(q, r) \in \mathbb{Z} \times \llbracket 0; k-1 \rrbracket$  tel que  $\alpha - \beta = qk + r$ . On en conclut que

$$ab^{-1} = x^{\alpha-\beta} = x^{qk+r} = (x^k)^q x^r$$

Or l'ordre de  $x$  est  $k$  c'est à dire  $x^k = 1$  donc

$$ab^{-1} = x^r \text{ avec } r \in \llbracket 0; k-1 \rrbracket$$

donc  $ab^{-1} \in H$ .

On en déduit que  $H$  est un sous-groupe de  $G$ .

De  $\text{Card } H = k$  et du théorème de Lagrange, on déduit que  $k \mid \text{Card } G$ . De plus

$$x^n = x^{k \frac{n}{k}} = \left(x^k\right)^{\frac{n}{k}} = 1^{\frac{n}{k}} = 1$$

II.A.4.b. L'anneau  $(\mathbb{Z}/p\mathbb{Z}, +, \times)$  étant un corps, puisque  $p$  est premier, on en déduit que  $(\mathbb{Z}/p\mathbb{Z})^*, \times$  est un groupe d'ordre  $p-1$ . D'après la question précédente, on peut conclure que

$$\forall \dot{x} \in (\mathbb{Z}/p\mathbb{Z})^* \quad \dot{x}^{p-1} = \dot{1}$$

ce qui est équivalent à

$$\forall x \in \mathbb{N} \quad p \nmid x \implies p \mid (x^{p-1} - 1)$$

### B) Etude du groupe $(\mathbb{Z}/n\mathbb{Z})^*, \times$ quand $n$ est premier

II.B.1. Tout élément de  $(\mathbb{Z}/n\mathbb{Z})^*$  possédant un ordre et un seul, on en déduit que la famille  $(\{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid x \text{ est d'ordre } d\})_{d \in D_{n-1}}$  forme une partition de  $(\mathbb{Z}/n\mathbb{Z})^*$ . Ainsi

$$\sum_{d \in D_{n-1}} \text{Card} \{x \in (\mathbb{Z}/n\mathbb{Z})^* \mid x \text{ est d'ordre } d\} = \text{Card} (\mathbb{Z}/n\mathbb{Z})^*$$

d'où

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

II.B.2.a. Soit  $k \in \llbracket 0; k-1 \rrbracket$ . Alors

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

Ainsi, l'ensemble  $\{\dot{1}, \dot{a}, \dots, \dot{a}^{k-1}\}$  est inclus dans l'ensemble des racines de  $X^d - 1$ . De plus, ce polynôme étant de degré  $d$ , on déduit de la question II.A.3.a. que l'ensemble précédent est exactement l'ensemble des racines de  $X^d - 1$ .

II.B.2.b. L'ordre de  $\dot{a}^k$  divise l'ordre de  $\dot{a}$  (car le groupe engendré par  $\dot{a}^k$  est un sous-groupe de celui engendré par  $\dot{a}$ ). Supposons que l'ordre de  $\dot{a}^k$  soit égal à  $d$  et posons  $\alpha = k \wedge d$ . On a  $\left(\dot{a}^k\right)^{\frac{d}{\alpha}} = \left(\dot{a}^d\right)^{\frac{k}{\alpha}} = \dot{1}$  donc  $d \mid_{\alpha} \frac{d}{\alpha} < d$  (car  $\alpha > 1$ ) ce qui est absurde. Ainsi l'ordre de  $\dot{a}^k$  est strictement inférieur à  $d$ .

II.B.2.c. Soit  $a$  un élément d'ordre  $d$ . Alors tous les éléments d'ordre  $d$  sont dans le sous-groupe engendré par  $a$  d'après la question II.B.2.a. et d'après la question précédente les éventuels  $\dot{a}^k$  d'ordre  $d$  sont ceux pour lesquels  $k \wedge d = 1$  (c'est à dire pour  $k \in S_d$ ). Ainsi, il y a au plus  $\phi(d)$  éléments d'ordre  $d$  donc  $\zeta(d) \leq \phi(d)$ .

On a

$$\sum_{d \in D_{n-1}} \phi(d) = n - 1 \implies \sum_{d \in D_{n-1}} (\phi(d) - \zeta(d)) = 0$$

Or pour tout  $d \in D_{n-1}$ , on a  $\phi(d) - \zeta(d) \geq 0$ . Et puisque une somme nulle de termes positifs ou nuls implique que chacun des termes est nul, on déduit que

$$\forall d \in D_{n-1} \quad \phi(d) = \zeta(d)$$

En particulier  $\zeta(n-1) = \phi(n-1) \neq 0$  (car  $n \geq 3$ ) donc il existe un élément  $\dot{b}$  d'ordre  $n-1$ . Ainsi le sous-groupe de  $(\mathbb{Z}/n\mathbb{Z})^*$  engendré par  $\dot{b}$  est d'ordre  $n-1 = \text{Card}(\mathbb{Z}/n\mathbb{Z})^*$  donc  $(\mathbb{Z}/n\mathbb{Z})^*$  est engendré par  $\dot{b}$ .

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

II.C.1. On a, d'après la formule du binôme de Newton,

$$(b+p)^{p-1} = \sum_{k=0}^{p-1} C_{p-1}^k b^{p-1-k} p^k = b^{p-1} + (p-1)b^{p-2}p = b^{p-1} - pb^{p-2} \quad [p^2]$$

Si  $(b+p)^{p-1} \equiv 1 \quad [p^2]$  et  $b^{p-1} \equiv 1 \quad [p^2]$ , alors  $pb^{p-2} \equiv 0 \quad [p^2]$  et donc  $p^2 | pb^{p-2}$  d'où  $p | b^{p-2}$  ce qui est absurde puisque  $\dot{b} \in (\mathbb{Z}/n\mathbb{Z})^*$  (donc  $\dot{b} \neq 0$ ).

Ainsi l'un au moins des deux entiers  $(b+p)^{p-1}$  et  $b^{p-1}$  n'est pas congru à 1 modulo  $p^2$ .

II.C.2. On procède par récurrence sur  $r \in \mathbb{N}$

- amorce :  $r = 0$  : on a  $c^{p-1} \equiv b^{p-1} \quad [p]$  donc  $c^{p-1} \equiv 1 \quad [p]$  ce qui implique qu'il existe un entier  $k_0$  tel que  $c^{p-1} = 1 + k_0 p$ . De plus  $k_0$  n'est pas divisible par  $p$  car sinon  $c^{p-1} \equiv 1 \quad [p^2]$  ce qui n'est pas le cas.

- hérédité : on suppose la propriété vraie au rang  $r$ . On a

$$c^{p^r(p-1)} = 1 + k_r p^{r+1} \text{ et } k_r \wedge p = 1$$

On a

$$\begin{aligned} c^{p^{r+1}(p-1)} &= (1 + k_r p^{r+1})^p \\ &= \sum_{i=0}^p C_p^i k_r^i p^{(r+1)i} \\ &= 1 + pk_r p^{r+1} + \sum_{i=2}^p C_p^i k_r^i p^{(r+1)i} \\ &= 1 + p^{r+2} \left( k_r + \sum_{i=2}^p C_p^i k_r^i p^{(r+1)(i-1)-1} \right) \end{aligned}$$

Or

$$\sum_{i=2}^p C_p^i k_r^i p^{(r+1)(i-1)-1} \equiv 0 \quad [p]$$

donc on pose

$$k_{r+1} = k_r + \sum_{i=2}^p C_p^i k_r^i p^{(r+1)(i-1)-1} \equiv k_r \not\equiv 0 \quad [p]$$

et comme  $k_{r+1} \not\equiv 0 \quad [p]$  est équivalent à  $k_{r+1} \wedge p = 1$  (car  $p$  est premier), la propriété est démontrée au rang  $r+1$ .

Ainsi  $c^{p^{\alpha-1}(p-1)} = 1 + k_{\alpha-1} p^\alpha \equiv 1 \quad [p^\alpha]$  donc  $c \in (\mathbb{Z}/n\mathbb{Z})^*$ .

II.C.3.a. Le cardinal de  $(\mathbb{Z}/n\mathbb{Z})^*$  est  $\phi(p^\alpha) = p^{\alpha-1}(p-1)$  donc  $r | p^{\alpha-1}(p-1)$ .

De plus le groupe engendré par  $c^{p^{\alpha-1}}$  est un sous-groupe de celui engendré par  $c$  donc l'ordre de  $c^{p^{\alpha-1}}$  (que l'on notera  $d$ ) divise  $r$ . Puisque  $\text{Card}(\mathbb{Z}/n\mathbb{Z})^* = p^{\alpha-1}(p-1)$ , alors  $d | p-1$ . On a

$$c^{p^{\alpha-1}} \equiv b^{p^{\alpha-1}} \equiv b \quad [p] \text{ (car } c \equiv b \quad [p])$$

donc

$$c^{p^{\alpha-1}d} \equiv b^d \pmod{p}$$

Or  $c^{p^{\alpha-1}d} \equiv 1 \pmod{p^\alpha}$  implique  $c^{p^{\alpha-1}d} \equiv 1 \pmod{p}$  donc  $b^d \equiv 1 \pmod{p}$ . On en conclut que  $p-1|d$  et donc que  $d = p-1$ . Puisque  $d|r$ , on en déduit pour finir que  $p-1|r$ .

II.C.3.b. On a

$$p-1|r \iff \exists a \in \mathbb{N} \quad r = a(p-1)$$

et puisque  $r|p^{\alpha-1}(p-1)$ , on en déduit que  $a|p^{\alpha-1}$  puis que  $a = p^\beta$  avec  $\beta \in \llbracket 0; \alpha-1 \rrbracket$ . Donc  $r = p^{\beta-1}(p-1)$  avec  $\beta \in \llbracket 0; \alpha-1 \rrbracket$ .

II.C.3.c. On a tout d'abord

$$c^r = cp^{\beta-1}(p-1) = 1 + k_\beta p^{\beta+1}$$

Supposons que  $\beta < \alpha-1$ . Alors on a  $\beta+1 < \alpha$ . Puisque  $k_\beta \wedge p = 1$  alors  $k_\beta p^{\beta+1} \not\equiv 0 \pmod{p}$  donc  $c^r \not\equiv 1 \pmod{p}$  ce qui est contradictoire donc  $\beta = \alpha-1$ . Ainsi  $c$  est d'ordre  $p^{\alpha-1}(p-1)$  donc est un générateur de  $(\mathbb{Z}/n\mathbb{Z})^*$ .

II.C.3.d. On vérifie aisément que  $\mathring{3}$  est un générateur de  $(\mathbb{Z}/7\mathbb{Z})^*$ , on pose donc  $b = 3$ . Puisque  $b^6 \equiv 43 \not\equiv 1 \pmod{49}$ , on déduit de la question précédente que  $\mathring{3}$  est un générateur de  $(\mathbb{Z}/49\mathbb{Z})^*$ .

## Partie III

III.1.a. Le nombre  $p$  étant premier et  $a \wedge p = 1$ , on a  $a^{p-1} \equiv 1 \pmod{p}$ . Ainsi  $a^{\frac{p-1}{2}}$  est racine du polynôme  $X^2 - 1$  n'admettant que deux racines à savoir 1 et  $-1$ . On en déduit immédiatement que  $a^{\frac{p-1}{2}} = \pm 1 \pmod{p}$ .

III.1.b. Soit  $a$  premier avec  $p$ . Montrons par récurrence sur  $t \in \llbracket 1; s \rrbracket$  que la propriété suivante est vraie

$$a^{q \times 2^{s-t}} \equiv 1 \pmod{p} \quad \text{ou} \quad \exists r \in \llbracket 1; t \rrbracket \quad a^{q \times 2^{s-r}} \equiv -1 \pmod{p}$$

- amorce :  $t=1$  : on a  $a^{\frac{p-1}{2}} = a^{q \times 2^{s-1}} \equiv \pm 1 \pmod{p}$  donc la propriété est vraie au rang 1
- hérédité : supposons la propriété vraie au rang  $t$ . Si  $a^{q \times 2^{s-t}} \equiv 1 \pmod{p}$  alors  $a^{q \times 2^{s-(t+1)}}$  est racine du polynôme  $X^2 - 1$  donc  $a^{q \times 2^{s-(t+1)}} \equiv \pm 1 \pmod{p}$  et la propriété est donc démontrée au rang  $t+1$ .

Or la propriété précédente au rang  $s$  est équivalente à  $H_a(p)$  donc  $H_a(p)$  est vérifiée pour  $a \wedge p = 1$ .

III.2. Si  $a \wedge p > 1$ , alors  $a$  et  $p$  ne sont pas premiers entre eux, donc  $a$  n'est pas inversible dans  $\mathbb{Z}/p\mathbb{Z}$ . Or si  $p$  était  $a$ -ppf alors il existerait  $\lambda$  tel que  $a^\lambda \equiv 1 \pmod{p}$  (en prenant  $\lambda = q$  ou  $\lambda = 2 \times q2^r$ ) ce qui signifierait que  $a \in (\mathbb{Z}/p\mathbb{Z})^*$  d'où une contradiction. Ainsi  $p$  ne peut être  $a$ -ppf.

III.3.a. Dans un premier temps, on détermine  $q$  et  $s$  tels que  $p-1 = q2^s$  avec  $q$  impair. Dans un second temps, on calcule itérativement  $a^q \pmod{p}$ . Si ce dernier est différent de 1  $\pmod{p}$ , on élève  $a^q$  au carré, et ainsi de suite...

Nous obtenons l'algorithme suivant (écrit en français avec une syntaxe proche de celle du C)

fonction *est-a-ppf* (*entier a*, *entier p*) **retourne booléen**

```

{
  /**déclaration des variables**
  entier q,s,α,k,r;
  \*****

  \***détermination de q et s***
  q ←(p - 1)/2;
  s ←1;
  tant que (q % 2 == 0) faire
  {
    q ←q/2;
    s ←s + 1;
  }
  \*****

  \*****calcul de aq [p]*****
  α ←1;
  pour (k = 1;k ≤ q;k ←k + 1) faire
  {
    α ←(α × a) % p;
  }
  \*****

  \*****p est-il a-ppf?*****
  si (α == 1) alors retourner VRAI;
  r ←0;
  tant que ((α != p - 1)&&(r < s)) faire
  {
    α ←(α × α) % p;
    r ←r + 1;
  }
  si (α = p - 1) alors retourner VRAI
  sinon retourner FAUX;
  \*****
}

```

III.3.b. A l'aide de l'algorithme précédent et de la machine, on obtient

<i>p</i>	49	91	111	121	135	1225
<i>a</i>	30	74	28	94	43	999
<i>p</i> est <i>a</i> -ppf	oui	oui	non	oui	non	oui

III.3.c. On a, par calcul,  $50^0 \equiv 1$  [561],  $50^1 \equiv 50$  [561],  $50^2 \equiv 256$  [561],  $50^3 \equiv 458$  [561],  $50^4 \equiv 460$  [561],  $50^5 \equiv 560$  [561],  $50^6 \equiv 511$  [561],  $50^7 \equiv 103$  [561],  $50^8 \equiv 101$  [561]. Par conséquent, l'ensemble donné est le sous-groupe de  $(\mathbb{Z}/561\mathbb{Z})^*$  engendré par 50.

# Partie IV

## A) Nombres de Carmichael

IV.A.1. On a

$$\forall i \in \llbracket 1; k \rrbracket \quad a^{n-1} = (a^{p_i-1})^{\frac{n-1}{p_i-1}} \equiv 1^{\frac{n-1}{p_i-1}} \equiv 1 \quad [p_i]$$

donc

$$\forall i \in \llbracket 1; k \rrbracket \quad p_i | a^{n-1} - 1$$

Et puisque les  $p_i$  sont premiers, on déduit que  $n | a^{n-1} - 1$  donc que  $a^{n-1} \equiv 1 [n]$ .

Comme  $561 = 3 \times 11 \times 17$  et  $2|560$ ,  $10|560$  et  $16|560$ , on en déduit que 561 est un nombre de Carmichael.

Comme  $10585 = 5 \times 29 \times 73$  et  $4|10584$ ,  $28|10584$  et  $72|10584$ , on en déduit que 10585 est un nombre de Carmichael.

IV.A.2.a. On a  $\text{Card}(\mathbb{Z}/n\mathbb{Z})^* = 2^{\alpha-1}$ . Le nombre  $a$  étant impair, il est alors premier avec  $n$  ainsi  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ . L'ordre de  $a$  divise  $2^{\alpha-1}$  donc est pair. Puisque  $2^\alpha - 1$  est impair, l'ordre de  $a$  ne peut diviser  $2^\alpha - 1$  donc si  $a \not\equiv 1 [n]$  alors  $a^{2^{\alpha-1}} \not\equiv 1 [n]$ .

On peut conclure qu'il n'existe pas de nombre de Carmichael de la forme  $2^\alpha$ .

IV.A.2.b.(i). Montrons par récurrence sur le nombre  $k$  de facteurs premiers de  $n$  que  $S_n$  est en bijection avec  $S_{p_1^{\alpha_1}} \times \dots \times S_{p_k^{\alpha_k}}$ .

– amorce :  $k = 2$  : cela a été déjà fait à la question I.4.

– hérédité : supposons la propriété vraie au rang  $k - 1$ . Soit  $n = \prod_{i=1}^k p_i^{\alpha_i} = p_k^{\alpha_k} \prod_{i=1}^{k-1} p_i^{\alpha_i}$ .

Compte tenu du fait que

$$p_k^{\alpha_k} \wedge \prod_{i=1}^{k-1} p_i^{\alpha_i} = 1 \text{ car les } p_i \text{ sont premiers}$$

on a, d'après la question I.4.,

$$S_n \cong S_{p_k^{\alpha_k}} \times S_{\prod_{i=1}^{k-1} p_i^{\alpha_i}}$$

On peut appliquer l'hypothèse de récurrence à  $\prod_{i=1}^{k-1} p_i^{\alpha_i}$  et on obtient alors

$$\begin{aligned} S_n &\cong S_{p_k^{\alpha_k}} \times S_{p_1^{\alpha_1}} \times \dots \times S_{p_{k-1}^{\alpha_{k-1}}} \\ &\cong^{h_n} S_{p_1^{\alpha_1}} \times \dots \times S_{p_k^{\alpha_k}} \end{aligned}$$

La propriété est donc vraie au rang  $k$

Soit donc  $t \in \mathbb{Z}$  tel que

$$t \equiv h_n^{-1}(\omega, 1, \dots, 1) [n]$$

De plus,  $t$  étant dans  $(\mathbb{Z}/n\mathbb{Z})^*$ , il est premier avec  $n$  et puisque  $n$  est un nombre de Carmichael, on en déduit que

$$t^{n-1} \equiv 1 [n]$$

IV.A.2.b.(ii). Ayant  $t^{n-1} \equiv 1 [n]$ , on a  $t^{n-1} \equiv 1 [p_1^{\alpha_1}]$  donc  $\omega^{n-1} \equiv 1 [p_1^{\alpha_1}]$ . Puisque  $\omega$  est

un générateur de  $(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^*$ , il est d'ordre  $\phi(p_1^{\alpha_1}) = p_1^{\alpha_1-1}(p_1 - 1)$ . Ainsi  $p_1^{\alpha_1-1}(p_1 - 1)$  divise  $n - 1$ . De plus, il existe un entier  $q$  tel que  $n = qp_1^{\alpha_1-1}(p_1 - 1) + 1$ . Puisque  $p_1^{\alpha_1-1}|n$ , on en déduit que  $p_1^{\alpha_1-1}|1$  ce qui implique que  $\alpha_1 = 1$  puis que  $p_1 - 1|n - 1$ .

IV.A.2.b.(iii). Si  $n$  est pair, alors  $n - 1$  est impair, et si  $p_1$  est impair alors  $p_1 - 1$  est pair. Ainsi, si  $n$  est pair  $p_1 - 1$  ne peut diviser  $n - 1$  donc  $n$  est impair. Le raisonnement fait en (i) et (ii) reste valable pour  $p_2, \dots, p_k$  donc

$$\forall i \in \llbracket 1; k \rrbracket \quad p_i - 1 | n - 1$$

On en déduit que  $n$  est un nombre de Carmichäel si et seulement si  $n = p_1 \dots p_k$  où les  $p_i$  sont des entiers premiers impairs deux à deux distincts et tels que  $\forall i \in \llbracket 1; k \rrbracket \quad p_i - 1 | n - 1$ .

IV.A.3. Par définition des nombres de Carmichäel  $n$  ne peut être un nombre premier. Supposons donc que  $n = pq$  est un nombre de Carmichäel avec  $p \neq q$ . Alors  $a^{pq-1} \equiv 1 [pq]$  pour  $a \wedge pq = 1$ . Or  $a^{pq-1} \equiv 1 [pq]$  implique que  $a^{pq-1} \equiv 1 [p]$  et puisque  $p$  est premier  $a^p \equiv a [p]$ , on a  $a^{pq-1} \equiv a^{q-1} [p]$ , donc  $a^{q-1} \equiv 1 [p]$ . Ainsi, on en déduit que  $p - 1 | q - 1$ . De même, on montre que  $q - 1 | p - 1$ . On en conclut que  $p - 1 = q - 1$  donc que  $p = q$  ce qui constitue une contradiction.

Par conséquent, un nombre de Carmichäel admet au moins trois facteurs premiers.

IV.A.4. Regardons l'équation modulo 85 et modulo 16 :

$$\begin{cases} 85p - 16k = 1 & \implies & -16k \equiv 1 \quad [85] & \text{donc } k \equiv (-16)^{-1} \equiv 69 \quad [85] \\ 85p - 16k = 1 & \implies & 85p \equiv 1 \quad [16] & \text{donc } p \equiv 85^{-1} \equiv 13 \quad [16] \end{cases}$$

Donc  $k \in (69 + 85\mathbb{Z})$  et  $p \in (13 + 16\mathbb{Z})$ .

Réciproquement, supposons que  $(k, p) \in (69 + 85\mathbb{Z}) \times (13 + 16\mathbb{Z})$ . On a alors

$$85(13 + 16\alpha) - 16(69 + 85\beta) = 1 + 1360(\alpha - \beta)$$

On en déduit que les solutions de l'équation sont de la forme  $(69 + 85n, 13 + 16n)$  avec  $n \in \mathbb{Z}$ .

Soit  $n = 5 \times 17 \times p_1 \dots p_i = 85p$  un nombre de Carmichäel,  $n - 1$  est alors divisible par 16 donc il existe un entier  $k$  tel que  $n - 1 = 16k$  et on en déduit que

$$85p - 16k = 1$$

De ce qui précède, on déduit

$$\exists \alpha \in \mathbb{Z} \quad p = 13 + 16\alpha \text{ et } k = 69 + 85\alpha$$

Puisque l'on cherche le plus petit  $n$  possible, il suffit de prendre  $\alpha = 0$  donc  $p = 13$  et  $k = 69$ . Ainsi  $n = 1105$  et on vérifie aisément que  $4|1104$ ,  $16|1104$  et  $12|1104$ .

On en conclut que 1105 est le plus petit nombre de Carmichäel divisible par  $5 \times 17$ .

## B) Test de Miller-Rabin

IV.B.1. Soit  $a$  un entier premier avec  $n$  (que l'on suppose impair) tel que  $n$  soit  $a$ -ppf. Il existe alors un entier  $d$  qui soit un diviseur strict de  $n - 1$  tel que  $a^d \equiv \pm 1 [n]$ , et en

élevant le tout à la puissance  $\frac{n-1}{d}$  (qui est pair), on en déduit que  $a^{n-1} \equiv 1 [n]$ . Si cette relation était vraie pour tout  $a \in (\mathbb{Z}/n\mathbb{Z})^*$  alors  $n$  serait soit premier soit un nombre de Carmichael ce qui est contradictoire avec les hypothèses faites sur  $n$ . Ainsi, il existe  $a \in (\mathbb{Z}/n\mathbb{Z})^*$  tel que  $n$  ne soit pas  $a$ -ppf.

IV.B.2. On suppose  $n$  composé. Puisque

$$\text{Card} \{a \in \mathbb{Z}/n\mathbb{Z} \mid n \text{ est } a\text{-ppf}\} < \phi(n)$$

on en déduit que la probabilité d'avoir  $a \in \{1, \dots, n-1\}$  tel que  $n$  soit  $a$ -ppf est majorée par  $\frac{\phi(n)}{n-1}$ . L'épreuve étant répétée  $k$  fois, on a

$$P(\text{"}n \text{ est déclaré premier"}) < \left(\frac{\phi(n)}{n-1}\right)^k$$