Royaume du Maroc
المملكة المغربية

Minitère de l'Education Nationale,
du Préscolaire et des Sports
وزارة التربية الوطنية والتعليم
الأولي والرياضة

Académie Hassan II
des Sciences et Techniques
أكاديمية الحسن الثاني
للعلوم و التقنيات

Juillet 2014 | Sujet de Mathématiques | Durée : 4h

Le sujet de l'épreuve de mathématiques du concours général des sciences et techniques, session 2015, est composé d'un problème consitité de 4 parties interdépendantes.
Pour répondre à une question de ce problème, tout candidat peut admettre et utiliser les résultats des questions qui la précédent, même si ne l'ai a pas traité, à condition d'indiquer avec précision les références des questions utilisées
Il est à noter que la qualité de la rédaction et de la présentation, la clarté et la précision des raisonnements constitueront des éléments importants pour l'appréciation des copies. Il convient en particulier de mentionner les références des questions abordées.

L'usage de tout document ou matériel électronique est interdit

Si au cours de l'épreuve, un candidat repère ce qui lui semble être une erreur d'énoncé, il le signale sur sa copie et poursuit sa composition en expliquant les raisons des initiatives qu'il est amené à prendre.

Notation, définitions et rappels :

- **Coefficient binomial :**
  Pour tout $n \in \mathbb{N}$ et tout $k \in \{0, 1, \ldots, n\}$, on définit : $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ le coefficient binomial usuel.
  Par convention, on pose $\binom{r}{k} = 0$ si $k > r$.
- Pour p et q deux nombres premiers, on note le plus grand commun diviseur de p et q par $p \wedge q$.
- Pour tout nombre naturel n non nul, on note $\varphi(n)$ le cardinal de l'ensemble des entiers k appartenant à $1, \ldots, n$ tels que $k \wedge n = 1$:
  $$\varphi(n) = \text{Card}\,\{k \in \{1, \cdots, n\} \mid k \wedge n = 1\}$$
  La fonction $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ est appelée la fonction indicatrice d'Euler.
- Pour tout entier naturel n, on note $\mathbb{Z}_n$ l'ensemble des classes de congruence modulo n. On rappelle que :
  $$\mathbb{Z}/n\mathbb{Z} = \left\{\bar{0}, \bar{1}, \cdots, \overline{n-1}\right\}$$
  On note $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ l'anneau de congruence modulo n, par $\mathbb{Z}_n$, et on rappelle que les lois $+$ et $\times$ définies par :
  $$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \times \bar{b} = \overline{ab}, \quad (a, b) \in \mathbb{Z}^2$$
  On pose :
  $$\mathbb{Z}_n^* = \left\{\bar{a} \in \mathbb{Z}_n \mid \exists \bar{b} \in \mathbb{Z}_n\,,\ \bar{a} \times \bar{b} = \bar{1}\right\}$$
  Autrement dit, $\mathbb{Z}_n^*$ est l'ensemble des éléments inversibles dans l'anneau $\mathbb{Z}_n$, c'est-à-dire ceux qui possèdent un inverse pour la multiplication modulo n.

Partie 1 :

Questions d'introductives sur la fonction indicatrice d'Euler

1.1. Calculer $\varphi(1), \varphi(13)$ et $\varphi(20)$.

1.2. Soit $n \in \mathbb{N} \setminus \{0, 1\}$, montrer que $\varphi(n) = n - 1$ si et seulement si n est un nombre premier.

1.3. Soit p un nombre premier.

1.3.1. Soient k et m deux entiers naturels non nuls, montrer que $m \wedge p^k \neq 1$ si et seulement si p divise m.

1.3.2. Déduire que $\varphi(p^n) = p^n - p^{n-1}$ pour tout entier n de $\mathbb{N}^*$.

L'objectif de cette partie est de présenter certaines propriétés de la fonction indicatrice d'Euler en utilisant le calcul des probabilités.
Considérons un entier naturel n qu'on décompose en produit d'entiers premiers sous la forme : $n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$, où $\alpha_1, \cdots, \alpha_r$ sont des entiers naturels non nul, et $p_1, \cdots, p_r$ sont des nombres premiers deux à deux distincts, et $r \geq 2$.
On considère une boîte contenant n boules numérotées de 1 à n. On tire une boule au hasard dans cette boîte, en supposant que les boules sont indistinguables au toucher.

1.4. Pour chaque $k \in 1, \ldots, r$, on considère l'événement A_k défini par :

$$A_k : \text{“La boule tirée porte un numéro multiple de } p_k \text{”}$$

On note $P(A_k)$ la probabilité de l'événement A_k.

1.4.1. Montrer que pour tout $k \in 1, \cdots, r$, on a $P(A_k) = \dfrac{1}{p_k}$.

1.4.2. Montrer que pour tout $k \in 2, \cdots, r$ et pour tout sous-ensemble $i_1, \ldots, i_k$ de l'ensemble $1, \ldots, r$, on a :

$$P\left(A_{i_1} \cap \cdots \cap A_{i_k}\right) = P\left(A_{i_1}\right) \times \cdots \times P\left(A_{i_k}\right)$$

1.4.3. Pour chaque $k \in 1, \ldots, r$, on note $\overline{A_k}$ l'événement contraire de A_k. Montrer que :

$$P\left(\overline{A_{i_1}} \cap \cdots \cap \overline{A_{i_k}}\right) = P\left(\overline{A_{i_1}}\right) \times \cdots \times P\left(\overline{A_{i_k}}\right)$$

1.5. On considère l'événement A défini par :

$$A : \text{“Tirer une boule portant un numéro premier avec } n \text{”}$$

On note $P(A)$ la probabilité de A.

1.5.1. Montrer que : $P(A) = \dfrac{\varphi(n)}{n}$.

1.5.2. Montrer que $A = \overline{A_1} \cap \cdots \cap \overline{A_r}$, puis en déduire que :

$$\varphi(n) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$$

1.6. Soit $m \in \mathbb{N} \setminus \{0, 1\}$. Écrivons m sous la forme d'un produit de puissances de nombres premiers $n = p_1^{\alpha_1} \times \cdots \times p_s^{\alpha_s}$, où $\alpha_1, \ldots, \alpha_s$ sont des entiers naturels non nuls, et $p_1, \ldots, p_s$ sont des nombres premiers deux à deux distincts. Montrer que :

$$\varphi(m) = n \prod_{k=1}^{s} \left(1 - \frac{1}{p_k}\right)$$

1.7. Soit m_1 et m_2 deux nombres de $\mathbb{N} \setminus \{0, 1\}$:

1.7.1. On suppose que $m_1 \wedge m_2 = 1$, montrer que $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.

1.7.2. On pose $d = m_1 \wedge m_2$, calculer $\varphi(m_1 m_2)$ en fonction de $d, \varphi(m_1), \varphi(m_2)$ et $\varphi(d)$.

1.8. Soit X la variable aléatoire qui associe à chaque issue le nombre qui figure sur la boule tirée. Rappelons que $n \in \mathbb{N} \setminus 0, 1$.

1.7.1. Soient $a, m \in \mathbb{N}^*$ et d un diviseur de m. Montrer que :

$$a \wedge m = d \Longleftrightarrow \left(\exists k \in \mathbb{N}^*,\ a = kd,\ k \wedge \frac{m}{d} = 1\right)$$

1.7.2. Soit d un diviseur de n, posons $\Delta_d = \{a \in \{1, \cdots, n\} \mid a \wedge n = d\}$, montrer que $\text{Card}(\Delta_d) = \varphi\left(\dfrac{n}{d}\right)$.

1.7.3. Soit d un diviseur de n. Considérons l'événement C_d : “$X \wedge n = d$”.
On exprime $P(C_d)$ en fonction de d et n et de la formule précédente.

1.7.4. Déduire que :

$$\sum_{d|n} \varphi(d) = n \qquad \text{(Identité d'Euler)}$$

Partie 2 :

L'ordre multiplicatif d'un nombre

L'objectif de cette partie est de définir l'ordre multiplicatif d'un nombre, et d'étudier quelques applications.

2.1. Soit n un entier naturel non nul et a un élément de $\mathbb{Z}^*$. Montrer que :

$$\bar{a} \in \mathbb{Z}_n^* \iff n \wedge a = 1$$

2.2. Soit p un nombre premier. Montrer que : $\mathbb{Z}_p^* = \left\{\bar{1}, \cdots, \overline{(p-1)}\right\}$.

2.3. Montrer que $(\mathbb{Z}_n^*, \times)$ est un groupe de $\varphi(n)$ éléments (c'est-à-dire que son ordre est $\varphi(n)$).

2.4. Soit $a \in \mathbb{N}^*$ et $g \in \mathbb{Z}_n^*$ tels que a et g soient premiers entre eux. On pose $\bar{u}_1, \ldots, \bar{u}_{\varphi(n)} \in \mathbb{Z}_n^*$.

2.4.1. Montrer que pour tout entier $j \in 1, \ldots, \varphi(n)$, il existe un unique élément $i \in 1, \ldots, \varphi(n)$ tel que : $\bar{a} \times \bar{u}_j = \bar{u}_i$.

2.4.2. Déduire que $a^{\varphi(n)} \equiv 1[n]$ (théorème d'Euler).

2.5. Soit p un nombre premier. Montrer que pour tout entier naturel a tel que a soit premier avec p, on a : $a^{p-1} \equiv 1[p]$ (petit théorème de Fermat).

2.6. Soit n un entier naturel non nul, montrer que pour tout $a \in \mathbb{N}^*$, on a :

$$a \wedge n = 1 \iff \exists k \in \mathbb{N}^*,\ a^k \equiv 1[n]$$

2.7. Soit n un entier naturel non nul, a tel que $a \wedge n = 1$. On définit alors $w_n(a)$ par :

$$w_n(a) = \min\left\{k \in \mathbb{N}^* \mid a^k \equiv 1[n]\right\}$$

Le nombre $w_n(a)$ est appelé l'ordre multiplicatif de a modulo n, et est un élément non vide de $\mathbb{N}$.

2.7.1. Montrer que pour tout $r \in \mathbb{N}^*$, on a :

$$w_n(a) = r \iff \begin{cases} a^r \equiv 1[n], \\ \forall k \in \mathbb{N}^*,\ a^k \equiv 1[n] \implies r|k \end{cases}$$

2.7.2. Montrer que $w_n(a)$ divise $\varphi(n)$.

2.7.3. Montrer que si n est un nombre premier, alors $w_n(a)$ divise le nombre $n-1$.

2.7.4. Montrer que pour tout entier naturel non nul k on a : $w_n(a^k) = \dfrac{w_n(a)}{k \wedge w_n(a)}$.

2.8. Soient a et b deux entiers naturels premiers entre eux et avec n, on suppose que $a \wedge n = b \wedge n = 1$ et $w_n(a) \wedge w_n(b) = 1$. Montrer que : $w_n(ab) = w_n(a)w_n(b)$.

2.9. **1ère Application :** Soient p et q deux nombres premiers distincts. On souhaite que le nombre $3^p - 2^p$ soit divisible par q.

2.9.1. Montrer que $q \geq 5$.

2.9.2. Montrer qu'il existe $u \in \mathbb{N}^*$, tel que $u \wedge q = 1$ et $3 \equiv 2u[q]$, puis déduire que $w_q(u)|p$.

2.9.3. En déduire que $p|(q-1)$.

2.10. **2ème Application :**

2.10.1. Soit k un nombre entier naturel. Trouver tous les restes possibles de la division euclidienne de k^3 par 9.

2.10.2. Calculer $w_9(7)$, puis montrer qu'il n'existe aucun entier naturel n tel que le nombre $7^n + n^3$ soit divisible par 9.

2.11. **3ème Application :** Soit p un nombre premier différent de 2. On pose $m = \dfrac{p^p - 1}{p-1}$.

2.11.1. Montrer que m est un entier naturel impaire.

2.11.2. Soit q un nombre premier divisant m. Montrer que $p|(q-1)$ puis en déduire que q s'écrit sous la forme $q = 2lp + 1$, où $l \in \mathbb{N}^*$. Il est possible de montrer que $q \neq p$ et on pose $w_q(p)$.

2.11.3. Soit r un entier naturel impaire. Montrer que $p^p - 1$ n'est pas divisible par $rp + 1$.

Partie 3 :

Étude de $(\mathbb{Z}_n^*, \times)$ dans le cas $n = p^\alpha$, où p est nombre premier et $\alpha \in \mathbb{N}^*$

Dans cette partie, on note p un entier premier impair.

3.1. Soit n un élément de $\mathbb{N} \setminus \{0,1\}$, montrer que l'anneau $\mathbb{Z}_n$ est un corps si et seulement si n est un nombre premier.

3.2. Soient P et Q deux polynômes de degré n et m tels que $0 \leq m \leq n$, définis par :

$$\begin{cases} P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \displaystyle\sum_{k=0}^{n} a_k x^k \\ Q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 = \displaystyle\sum_{k=0}^{m} b_k x^k \end{cases}$$

où $a_n, a_{n-1}, \ldots, a_1, a_0$ et $b_m, \ldots, b_1, b_0$ sont des éléments de l'ensemble $\mathbb{Z}_p$.
Montrer que le produit PQ est un polynôme de degré $n+m$.

3.3. Soit $P(x)$ un polynôme de degré n tel que $2 \leq n$ avec $P(x) = \displaystyle\sum_{k=0}^{n} a_k x^k$ où $a_0, a_1, \ldots, a_n$ sont des éléments de $\mathbb{Z}_p$.

3.3.1. Soient α et β deux éléments distincts de $\mathbb{Z}_p$ et $k \in \mathbb{N}^*$. Montrer que la différence $\alpha^k - \beta^k$ peut s'écrire comme un produit de $(\alpha - \beta)$ par une somme de α et β.

3.3.2. Soit α un élément de $\mathbb{Z}_p$. Montrer que $P(\alpha) = 0$ si et seulement s'il existe un polynôme Q de degré $n-1$ à coefficients dans $\mathbb{Z}_p$ tel que : $P(x) = (x-\alpha)Q(x)$.

3.3.3. Montrer que le nombre de racines distinctes du polynôme P dans $\mathbb{Z}_p$ ne dépasse pas n.

3.4. Trouver dans l'anneau $\mathbb{Z}_6$ toutes les racines de la fonction $P(x) = x^2 - x$, puis trouver deux factorisations différentes de $P(x)$ sous la forme $P(x) = (x-\alpha)(x-\beta)$. Que peux-tu conclure en te référant à ce qui précède ?

Rappelons ici que l'ordre du groupe $(\mathbb{Z}_p^*, \times)$ est $\varphi(p) = p-1$ et que $\mathbb{Z}_p^* = \{1, 2, \cdots, (p-1)\}$.

3.5. Soient p et q des nombres premiers, et $\alpha \in \mathbb{N}^*$, tel que q^α divise $p-1$. Pour tout k de l'ensemble $\{1, \cdots, p-1\}$, on pose $y_k = k^{(p-1)/q^\alpha}$.

3.5.1. Montrer que $y_k^{q^\alpha} \equiv 1[p]$, et en déduire qu'il existe n_k de $\{0, \cdots, \alpha\}$ tel que $w_p(y_k) = q^{n_k}$.

3.5.2. Soit $m = \max\{n_k \mid k \in \{1, \ldots, p-1\}\}$, montrer que tous les éléments de l'ensemble Z_p^* sont des racines du polynôme $P(x) = x^{\frac{p-1}{q^\alpha}} - 1$, en déduire que $m = \alpha$.

3.6. Soit $p - 1 = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ la décomposition du nombre $p-1$ en un produit de nombres premiers, où $\alpha_1, \ldots, \alpha_s$ sont des entiers naturels non nuls, et $p_1, \ldots, p_s$ sont des nombres premiers distincts deux à deux.

3.6.1. Montrer que pour tout $i \in \{1, \ldots, s\}$, il existe $a_i \in \{1, \ldots, p-1\}$ tel que $w_p(a_i) = \frac{p-1}{p_i^{\alpha_i}}$, puis trouver un élément $a \in \mathbb{N}^*$ tel que $w_p(a) = p-1$ et $a \wedge p = 1$.

3.6.2. Montrer que $\mathbb{Z}_p^* = \{1, a, a^2, \ldots, a^{p-1}\}$, c'est-à-dire que pour tout $b \in \mathbb{Z}_p^*$, il existe $k \in \{0, 1, \ldots, p-1\}$ tel que $b = a^k$ (l'ordre de $(\mathbb{Z}_p^*, \times)$ est cyclique).

Soit a de $\mathbb{N} \setminus \{0,1\}$.

3.7. Montrer que pour tout $k \in \mathbb{N}^*$, il existe $\lambda_k \in \mathbb{N}^*$ tel que $p \wedge \lambda_k = 1$ et $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$.

3.8. En déduire que $w_{p^\alpha}(1+p) = p^{\alpha-1}$.

3.9. Vérifier qu'il existe $x \in \mathbb{N}^*$ tel que $w_p(x) = p-1$ et $p \wedge x = 1$.

3.10. Montrer que $p-1 | w_{p^\alpha}(x)$ et en déduire qu'il existe $x_1 \in \mathbb{N}^*$ tel que $p \wedge x_1 = 1$ et $w_{p^\alpha}(x_1) = p-1$.

3.11. Montrer qu'il existe $y \in \mathbb{N}^*$ tel que $w_{p^\alpha}(y) = p^{\alpha-1}(p-1)$ (l'ordre de $(\mathbb{Z}_{p^\alpha}^*, \times)$ est cyclique).

Partie 4 :

Concernant les nombres de Carmichael

Définition : Un nombre est dit de Carmichael, tout entier naturel n vérifiant :

- n n'est pas premier.
- Pour tout $k \in \mathbb{Z}^*$, tel que $k \wedge n = 1$, on a $k^{n-1} \equiv 1[n]$.

4.1. Soient $p_1, \cdots, p_s$ des nombres premiers impairs et distincts, avec $s \geq 3$. Posons $n = p_1 \cdots p_s$ et supposons que, pour tout $j \in \{1, \ldots, s\}$, on a $(p_j - 1) \mid (n-1)$. Montrer que n est un nombre de Carmichael.

4.2. Montrer que 561 est un nombre de Carmichael.

Soit n est un nombre de Carmichael, et on écrit la factorisation de n en nombres premiers $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, où $\alpha_1, \cdots, \alpha_r$ sont des entiers naturels non nuls, et $p_1, \cdots, p_r$ sont des nombres premiers distincts deux à deux.

4.4. Montrer que les nombres $p_1, \cdots, p_r$ sont impaires.

4.5. Soient $i \in \{1, \cdots, r\}$ et $a_i \in \mathbb{N} \setminus \{0,1\}$, tels que $a_i \wedge p_i = 1$ et $w_{p_i^{\alpha_i}}(a_i) = p_i^{\alpha_i - 1}(p_i - 1)$.

4.5.1. Justifier l'existence de a_i, et montrer qu'il existe $t \in \mathbb{N} \setminus \{0, 1\}$ tel que

$$\begin{cases} t \equiv a_i \ [p_i^{\alpha_i}], \\ t \equiv 1 \ [p_j^{\alpha_j}], \quad j \neq i. \end{cases}$$

4.5.2. Montrer que $p_i^{\alpha_i - 1}(p_i - 1) \mid (n-1)$ puis en déduire que $t^{n-1} \equiv 1 \ [n]$.

4.5.3. Montrer que $\alpha_i = 1$ et que $(p_i - 1) \mid (n-1)$.

4.5.4. Montrer que $3 \leq r$.

4.6. Résoudre dans $\mathbb{Z}^2$ l'équation $85x - 16y = 1$ à deux inconnues x et y, puis trouver le plus petit nombre de Carmichael divisible par 5 et 17.

Fin du sujet