Olympiades mathématiques de première 2020. Sujet national.

I Exercice pour tous les candidats : batailles navales.

Un joueur effectue une sorte de « bataille navale » sur un damier carré de $n \times n$ cases, avec $n \geqslant 3$. Un bateau est représenté par un rectangle constitué de trois cases de la taille des cases du damier. Il est placé horizontalement ou verticalement sur trois cases du damier.

Le bateau est invisible du joueur.

Le joueur effectue plusieurs tirs sur des cases distinctes du damier dans le but de toucher au moins une des cases occupées par le bateau.

On appelle « jeu optimal » un ensemble de tirs permettant de toucher le bateau à coup sûr, quelle que soit la position occupée par celui-ci, et comprenant le nombre minimal de tirs pour y parvenir.

On note $\mathsf{J}(n)$ le nombre de tirs réalisés dans un jeu optimal. Le but de cet exercice est de déterminer $\mathsf{J}(n)$ et de réaliser un jeu optimal effectif.

Partie A : étude de trois cas particuliers.

0. Cas où $n = 3$.

(a) Combien de positions différentes le bateau est-il susceptible d'occuper sur le damier ?

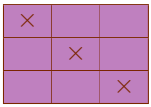
1	1	1
2	2	2
3	3	3

et

4	5	6
4	5	6
4	5	6

Le bateau peut occuper 6 positions sur le damier.

(b) Reproduire le damier sur la copie et indiquer trois cases sur lesquelles tirer pour que le bateau soit touché à coup sûr. On placera une croix ($\times$) dans chacune de ces cases.



(c) Montrer qu'on ne peut pas réaliser un jeu optimal avec deux tirs.

Le damier comporte 3 colonnes, donc avec 2 tirs une colonne (au moins) est épargnée et si le bateau est placé dans cette colonne il est sauf.

On ne peut pas réaliser un jeu optimal avec deux tirs.

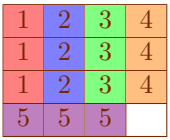
(d) En déduire que $J(3) = 3$.

D'après la question 0.(b) $J(3) \leqslant 3$ et, d'après la question 0.(c), $J(3) \geqslant 3$. Enfin

$J(3) = 3$.

1. Cas où $n = 4$.

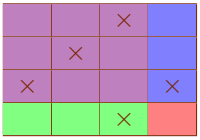
(a) Sur un damier 4×4, indiquer cinq positions pour le bateau qui n'ont aucune case en commun deux à deux. Que peut-on en déduire pour $J(4)$?



Cette configuration montre qu'il ne faut pas moins de 5 tirs pour réaliser un jeu optimal.

$J(4) \geqslant 5$.

(b) Représenter un jeu optimal à cinq tirs sur un damier 4×4. En déduire $J(4)$.

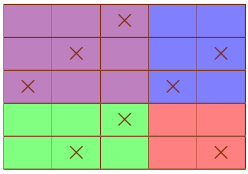


De la représentation ci-dessus nous déduisons que $J(4) \leqslant 5$.
En tenant compte du résultat de la question précédente nous en déduisons :

$$J(4) = 5.$$

2. Cas où $n = 5$. Montrer que $J(5) = 8$.

En procédant comme précédemment, $J(5) \leqslant 8$ car



permet de toucher à coup sûr, et $J(5) \geqslant 8$ car la configuration suivante nécessite au moins 8 tirs :

1	1	1	5	6
2	2	2	5	6
3	4		5	6
3	4	7	7	7
3	4	8	8	8

des deux précédentes inégalités nous déduisons :

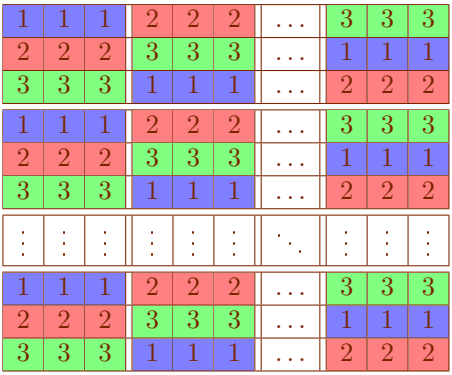
$$J(5) = 8.$$

Partie B : cas général.

1. Cas où $n = 3p$, avec p entier et $p \geqslant 1$.

   (a) Indiquer une façon de placer sur le damier un nombre maximal de positions disjointes deux à deux pouvant être occupées par le bateau. Que peut-on dire de $J(3p)$?

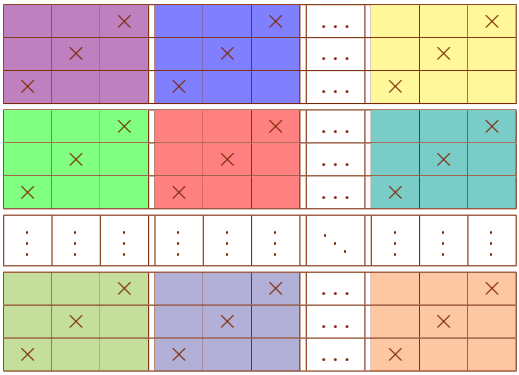
   Dans ce cas il est possible de recouvrir complètement le damier par des bateaux :



Puisque tout les $9p^2$ cases du damier sont recouvertes et que chaque bateau recouvre 3 cases nous avons placé $\frac{9p^2}{3} = 3p^2$ bateaux. Il faudra donc au minimum $3p^2$ coup pour toucher un bateau à coup sûr.

$$\mathsf{J}(3p) \geqslant 3p^2.$$

(b) En utilisant le schéma proposé en A1(b), expliquer comment réaliser un jeu optimal pour $n = 3p$.



Les tirs dessinés ci-dessus permettent à coup sûr de toucher un bateau placé sur le damier. Dénombrons les tirs ainsi dessinés.

Les tirs sont regroupés en petits damiers de taille 3×3 contenant chacun 3 tirs.

Il y a p petits damiers 3×3 alignés et autant superposés en colonnes donc au total il y a $p \times p$ petits damiers 3×3.

Il y a donc $3p^2$ tirs dessinés sur le damier ci-dessus.

$$\mathsf{J}(3p) \leqslant 3p^2.$$

(c) Montrer que $\mathsf{J}(3p) = 3p^2$.

Des deux questions précédentes nous déduisons :

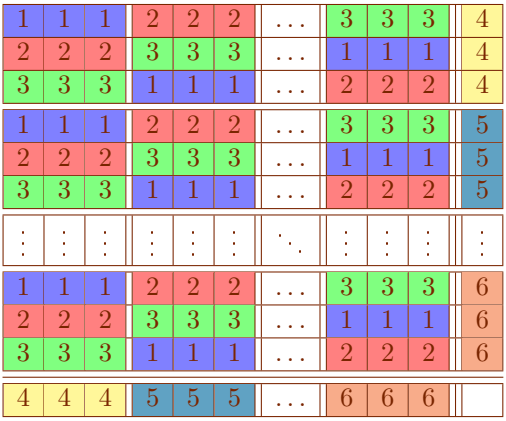
$$\mathsf{J}(3p) = 3p^2.$$

2. Cas où $n = 3p + 1$, avec p entier et $p \geqslant 1$.

(a) Combien peut-on placer au maximum sur le damier de positions du bateaux disjointes deux à deux ?

Le damier comporte $(3p+1)^2 = 9p^2+6p+1$ cases. Un bateau recouvrant 3 cases, le nombre maximum b de bateau vérifie donc $b \leqslant \frac{9p^2+6p+1}{3} = 3p^2 + 2p + \frac{1}{3}$. Donc : $b \leqslant 3p^2 + 2p$.

En procédant comme précédemment



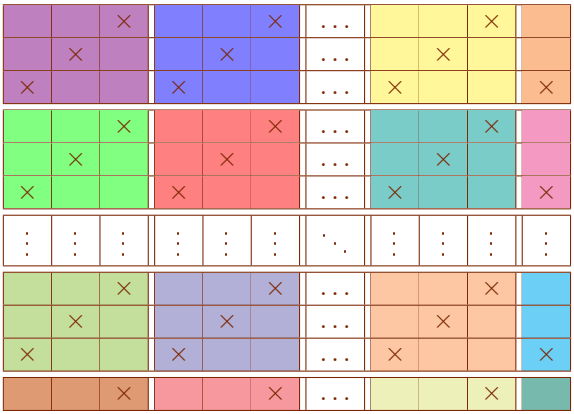
Au damier de la question précédente qui pouvait contenir $3p^2$ bateaux nous avons rajouté une colonne à droite et une ligne en dessous. Sur cette ligne et cette colonne nous avons dessiné $2 \times p$ bateaux. Le damier contient donc au total $3p^2 + 2p$ bateaux.

Ainsi le damier contient au plus $3p^2 + 2p$ bateaux et nous avons effectivement réussi à en placer $3p^2 + 2p$, autrement dit :

le nombre maximal de bateaux est $3p^2 + 2p$.

(b) Réaliser un jeu optimal pour $n = 3p+1$ en expliquant avec précision la démarche.

Reprenons les tirs que nous avions obtenus lorsque $n = 3p$ en ajoutant une ligne en dessous et une colonne à droite.



Le damier ci-dessus montre clairement qu'il est impossible de placer un bateau de trois cases qui ne soit pas sur une case de tir.

Sur ce damier sont dessinés les $3p^2$ tirs apparaissant déjà dans le cas $n = 3p$ auxquels s'ajoutent $2p$ tirs dessinés sur les ligne et colonne rajoutées.

D'après la question précédente $\mathrm{J}(3p+1) \geqslant 3p^2 + 2p$ et nous venons d'établir que $\mathrm{J}(3p+1) \leqslant 3p^2 + 2p$. Il est donc impossible d'obtenir des tirs touchant un navire à coup sûr de moins avec moins que $3p^2 + 2p$ tirs.

Le damier ci-dessus correspond à un jeu optimal.

(c) Que vaut $\mathrm{J}(3p+1)$?

Nous avons établit au cours de la question précédente que

$$\mathrm{J}(3p+1) = 3p^2 + 2p.$$

3. Recherche d'une caractérisation commune de $\mathrm{J}(n)$, pour tout entier $n \geqslant 3$.
On traite le cas $n = 3p+2$ par des raisonnements analogues à ceux des cas $n = 3p$ et $n = 3p+1$ et on obtient : $\mathrm{J}(3p+2) = 3p^2 + 4p + 1$.

(a) Montrer que, pour tout entier $n \geqslant 3$, $\mathrm{J}(n)$ est le plus grand entier inférieur ou égale à $\frac{n^2}{3}$.

Démontrons par disjonction des cas que, pour tout $n \geqslant 3$, $\mathrm{J}(n)$ est le plus grand entier inférieur ou égale à $\frac{n^2}{3}$.

Soit $n \in \mathbb{N}$ avec $n \geqslant 3$.

* Supposons que $n = 3p$ avec $p \in \mathbb{N}$.
  Alors : $\frac{n^2}{3} = \frac{(3p)^2}{3} = 3p^3 = \mathrm{J}(3p)$. Donc $\mathrm{J}(n)$ est bien le plus grand entier inférieur ou égale à $\frac{n^2}{3}$.
* Supposons que $n = 3p + 1$ avec $p \in \mathbb{N}$.
  Alors : $\frac{n^2}{3} = 3p^2 + 2p + \frac{1}{3}$ et $\mathrm{J}(n) = 3p^2 + 2p$.
  Donc : $J(n) \leqslant \frac{n^2}{3}$.
  De plus $\left|\frac{n^2}{3} - \mathrm{J}(n)\right| = \frac{1}{3} < 1$.
  Donc, là encore, $\mathrm{J}(n)$ est bien le plus grand entier inférieur ou égale à $\frac{n^2}{3}$.
* Supposons que $n = 3p + 2$ avec $p \in \mathbb{N}$.
  Alors : $\frac{n^2}{3} = 3p^2 + 4p + \frac{4}{3}$ et $\mathrm{J}(n) = 3p^2 + 4p + 1$.
  Donc : $J(n) \leqslant \frac{n^2}{3}$.
  De plus $\left|\frac{n^2}{3} - \mathrm{J}(n)\right| = \frac{4}{3} - 1 = \frac{1}{3} < 1$.
  Donc, là encore, $\mathrm{J}(n)$ est bien le plus grand entier inférieur ou égale à $\frac{n^2}{3}$.

En réunissant les trois cas :

> pour tout entier $n \geqslant 3$, $\mathrm{J}(n)$ est le plus grand entier inférieur ou égale à $\frac{n^2}{3}$.

(b) Existe-t-il un entier n tel que $\mathrm{J}(n) = 2020$?

Pour répondre à cette question il serait naturel de se lancer dans un raisonnement par analyse synthèse, mais ici aucune solution n'existe d'où le choix du raisonnement par l'absurde.

Raisonnons par l'absurde.

Supposons qu'il existe $n \in \mathbb{N}$ et $n \geqslant 3$ tel que $\mathrm{J}(n) = 2020$ et démontrons que cela conduit à une impossibilité.

Cas 1 : si $n = 3p$ alors $\mathrm{J}(n) = 3p^2$ et donc

$$\mathrm{J}(n) = 2020 \Leftrightarrow 3p^2 = 2020$$

Donc $p \notin \mathbb{N}$ et dans ce cas il n'y a pas d'entier n qui convienne.

Cas 2 : si $n = 3p + 1$, alors $\mathrm{J}(n) = 3p^2 + 2p$ et donc

$$\mathrm{J}(n) = 2020 \Leftrightarrow 3p^2 + 2p - 2020 = 0$$

La résolution de ce dernier trinôme ne conduit à aucune racine entière donc dans ce cas il n'y a pas d'entier n qui convienne.

Cas 3 : si $n = 3p + 1$, alors $\mathrm{J}(n) = 3p^2 + 4p + 1$ et donc

$$\mathrm{J}(n) = 2020 \Leftrightarrow 3p^2 + 4p - 2019 = 0$$

La résolution de ce dernier trinôme ne conduit à aucune racine entière donc dans ce cas il n'y a pas d'entier n qui convienne.

Dans tous les cas nous obtenons une impossibilité.

Nous avons démontré en raisonnant par l'absurde qu'il n'existe pas d'entier naturel n tel que $\mathrm{J}(n) = 2020$.

II Exercice pour les candidats de la voie générale en spécialité mathématiques : ensembles surprenants.

On désigne par $\mathbb{N}^*$ l'ensemble des entiers naturels non nuls.

Dans tout l'exercice, les ensembles considérés sont des sous-ensembles finis non vides de $\mathbb{N}^*$.

Si A est un tel ensemble, on désigne par $P(A)$ le produit des éléments de A et par $C(A)$ la somme des carrés des éléments de A.

Par exemple, si $A = \{1, 2, 5\}$, alors $P(A) = 1 \times 2 \times 5 = 10$ et $C(A) = 1^2 + 2^2 + 5^2 = 30$.

On dit qu'un ensemble A fini est *surprenant* si $P(A) = C(A)$.

0. Deux exemples.

(a) L'ensemble $\{1, 2, 3, 2020\}$ est-il surprenant ?

$$\begin{aligned} P(\{1, 2, 3, 2020\}) &= 1 \times 2 \times 3 \times 2020 \\ &= 12\,120 \end{aligned}$$

et :

$$\begin{aligned} C(\{1, 2, 3, 2020\}) &= 1^2 + 2^2 + 3^2 + 2020^2 \\ &= 4\,080\,414 \end{aligned}$$

$\{1, 2, 3, 2020\}$ n'est pas surprenant.

(b) L'ensemble $\{6, 15, 87\}$ est-il surprenant ?

$P(\{6, 15, 87\}) = 7830 = C(\{6, 15, 87\})$.

$\{6, 15, 87\}$ est surprenant.

1. On considère un sous-ensemble fini A de $\mathbb{N}^*$ tel que $P(A) \geqslant 5$.

(a) Quels sont les nombres x vérifiant l'égalité

$$xP(A) = P(A) - 1 + x^2 \ ?$$

Cette égalité permet vraisemblablement de démontrer que $P(A) - 1 \notin A$ mais je ne vois pas comment. Si vous avez une idée envoyez-moi un mail.

$$xP(A) = P(A) - 1 + x^2$$

équivaut successivement à :

$$\begin{aligned}
x^2 - P(A)x + P(A) - 1 &= 0 \\
\left(x^2 - 2\frac{P(A)}{2}x + \frac{P(A)^2}{4}\right) - \frac{P(A)^2}{4} + P(A) - 1 &= 0 \\
\left(x - \frac{P(A)}{2}\right)^2 - \left[\left(\frac{P(A)}{2}\right)^2 - 2 \times \frac{P(A)}{2} \times 1 + 1^2\right] &= 0 \\
\left(x - \frac{P(A)}{2}\right)^2 - \left(\frac{P(A)}{2} - 1\right)^2 &= 0 \\
(x-1)\left[x - (P(A) - 1)\right] &= 0 \\
x = 1 \quad \text{ou} \quad x &= P(A) - 1
\end{aligned}$$

L'ensemble des solutions de l'équation $xP(A) = P(A) - 1 + x^2$ est : $\mathscr{S} = \{1,\ P(A) - 1\}$.

(b) Montrer que le nombre $P(A) - 1$ n'appartient pas à A.

Démontrons que $P(A) - 1 \notin A$ en raisonnant par l'absurde.

Supposons que $P(A) - 1 \in A$ et démontrons que cela conduit à une contradiction.
Puisque $P(A) - 1 \in A$, $(P(A) - 1)$ divise $P(A)$. Donc il existe $n \in \mathbb{N}^*$ tel que $n(P(A) - 1) = P(A)$ ou encore $n = \frac{P(A)}{P(A)-1}$.
Considérons la fonction $f : \left\{ \begin{array}{ccc} [5;+\infty[& \to & \mathbb{R} \\ x & \mapsto & \frac{x}{x-1} \end{array} \right.$.
f est dérivable en tant que quotient de fonctions dérivables sur $[5;+\infty[$ et ne s'annulant pas sur$[5;+\infty[$. De plus, pour tout $x \in [5;+\infty[$:

$$\begin{aligned}
f'(x) &= \frac{x - 1 - x}{(x-1)^2} \\
&= -\frac{1}{(x-1)^2}
\end{aligned}$$

et donc :

$$f'(x) < 0$$

Par conséquent f est strictement décroissante et en particulier : de $P(A) \geqslant 5$ nous déduisons $f(P(A)) \leqslant f(5)$.

Autrement dit : $n = f(P(A)) \leqslant \frac{5}{4}$.
Donc, puisque $n \in \mathbb{N}^*$, $n = 1$. Or dans ce cas $P(A) - 1 = P(A)$ ce qui est impossible.

Nous avons démontré en raisonnant par l'absurde que $P(A) - 1 \notin A$.

(c) On note A' l'ensemble obtenu en ajoutant l'entier $P(A) - 1$ à l'ensemble A. En d'autres termes,

$$A' = A \cup \{P(A) - 1\}.$$

Exprimer $P(A') - C(A')$ en fonction de $P(A) - C(A)$.

$$\begin{aligned} P(A') - C(A') &= P(A) \times [P(A) - 1] - \left[C(A) + (P(A) - 1)^2\right] \\ &= P(A)^2 - P(A) - C(A) - P(A)^2 + 2P(A) - 1 \end{aligned}$$

Enfin

$$P(A') - C(A') = P(A) - C(A) - 1.$$

(d) En déduire que si $P(A) > C(A)$, on peut trouver un ensemble surprenant B contenant A.

Si $P(A) > C(A)$ alors $P(A') - C(A') = P(A) - C(A) - 1$ peut s'interpréter en disant que l'écart entre $P(A')$ et $C(A')$ est diminué de 1 par rapport à l'écart entre $P(A)$ et $C(A)$.

Notons $A_0 = A$, $A_1 = A'$, $A_2 = A_1 \cup \{P(A_1) - 1\}$, etc.
D'une part : $A_0 \subset A_1 \subset A_2 \subset \ldots$.
D'autre part, la suite $(P(A_i) - C(A_i))_i$ est une suite arithmétique de premier terme un entier naturel non nul et de raison -1. Il existera donc un rang pour lequel elle vaudra 0 : il existe $i_0 \in \mathbb{N}$ tel que $A_0 \subset A_{i_0}$ et $P(A_{i_0}) - C(A_{i_0}) = 0$.

Si $P(A) > C(A)$ il est possible de trouver un ensemble surprenant, B, contenant A.

(e) Trouver un ensemble surprenant contenant l'ensemble $\{3, 4, 9\}$.

Ensemble A	$P(A)$	$C(A)$	$P(A)-1$
$A_0 = \{3, 4, 9\}$	108	106	107
$A_1 = \{3, 4, 9, 107\}$	11556	11555	11555
$A_2 = \{3, 4, 9, 107, 11555\}$	133529580	133529580	

$\{3, 4, 9, 107, 11555\}$ est un ensemble surprenant contenant $\{3, 4, 9\}$.

2. On considère à nouveau un sous-ensemble fini A de $\mathbb{N}^*$ tel que $P(A) \geqslant 5$.

(a) Prouver que le nombre $P(A) - 2$ n'appartient pas à A.

Soit $g : \left\{ \begin{array}{ccc} [5;+\infty[& \to & \mathbb{R} \\ x & \mapsto & \frac{x}{x-2} \end{array} \right.$. En procédant comme à la question précédente nous établissons que g est strictement décroissante et comme $P(A) \geqslant 5$ nous en déduisons $g(P(A)) = \frac{P(A)}{P(A)-2} \leqslant \frac{5}{3}$. Or, si $P(A)-2 \in A$ alors $\frac{P(A)}{P(A)-2} \in \mathbb{N}^*$ donc, nécessairement $\frac{P(A)}{P(A)-2} = 1$. Ce qui est impossible.
Nous avons donc établi en raisonnant par l'absurde que :

$$P(A) - 2 \notin A.$$

(b) En déduire que si $P(A) < C(A)$, on peut trouver un ensemble surprenant B contenant A.

Notons $A_1 = A \cup \{P(A) - 2\}$.

$$\begin{aligned} P(A_1) - C(A_1) &= (P(A) - 2)P(A) - C(A) - [p(A) - 2]^2 \\ &= P(A)^2 - 2P(A) - C(A) - P(A)^2 + 4P(A) - 4 \\ &= P(A) - C(A) + P(A) + 4 \end{aligned}$$

Or $P(A) - C(A) < 0$ par hypothèse et $P(A) + 4 > 0$ donc :

$$P(A_1) - C(A_1) > P(A) - C(A)$$

En réitérant nous construirions une suite $(A_j)_j$ croissante au sens de l'inclusion : $A = A_0 \subset A_1 \subset A_2 \subset \ldots$ et telle que la suite $(P(A_j) - C(A_j))_j$ est strictement croissante.

Ainsi $(P(A_j) - C(A_j))_j$ est une suite strictement croissante d'entiers dont le premier terme est strictement négatif. Il existe donc un rang j_0 tel que $P(A_{j_0}) - C(A_{j_0}) > 0$.
À partir du rang j_0 nous retombons sur le cas étudié à la question 1 et nous pouvons donc affirmer :

> Si $P(A) < C(A)$ il est possible de trouver un ensemble surprenant, B, contenant A.

3. En déduire finalement que, pour tout sous-ensemble fini non vide A de $\mathbb{N}^*$, on peut trouver un ensemble surprenant B contenant A.

Si $5 \in A$, alors $P(A) \geqslant 5$ et nous pouvons utiliser les résultats précédentes.
Sinon $P(A \cup \{5\}) \geqslant 5$ et nous pouvons appliquer les résultats précédents au sur-ensemble $A \cup \{5\}$.
Bref, dans tous les cas

> il est possible de trouver un ensemble surprenant, B, contenant A.

4. Montrer qu'on peut trouver un ensemble surprenant ayant 67 éléments et contenant $A = \{1, 2, 5\}$.

Nous sommes dans le cas $P(A) \geqslant 0$ et $P(A) < C(A)$ (question 2). En effet :

Ensemble A	$P(A)$	$C(A)$	$P(A) - C(A)$
$A_0 = \{1, 2, 5\}$	10	30	-20
$A_1 = \{1, 2, 5, 8\}$	80	94	-14
$A_2 = \{1, 2, 5, 8, 78\}$	6240	6178	62

À partir de A_2 nous sommes dans le cas $P(A) > C(A)$ et en appliquant alors 62 fois le procédé vu à la question 1 nous pouvons construire une suite $A_2 \subset A_3 \subset \cdots \subset A_{64}$ en ajoutant à chaque étape un élément au précédent ensemble.
Ainsi $A_{64} = \{1, 2, 5, 8, 78, a_1, a_2, \ldots, a_{62}\}$ contient 67 éléments et par construction $P(A_{64}) - C(A_{64}) = 0$.

> Il est possible de trouver un ensemble surprenant ayant 67 éléments et contenant $\{1, 2, 5\}$.

III Exercice pour les candidats n'ayant pas suivi la spécialité de mathématiques de voie générale : mathématiques et cryptographie une longue histoire !

Partie A.

Le chiffre de César ou le chiffrement par décalage est une méthode de chiffrement très simple utilisée par Jules César dans ses correspondances secrètes. Le texte chiffré s'obtient en décalant chaque lettre d'un nombre fixe, appelé clé, dans l'ordre de l'alphabet.

Par exemple avec une clé de 3 vers la droite, A est remplacé par D, B devient E, et ainsi jusqu'à W qui devient Z, puis X devient A etc.

1. Coder le mot suivant avec la clef 3 : OLYMPIADES.

   Facilitons le déchiffrage en utilisant un tableau (décalage de 3).

Clair	a	b	c	d	e	f	g	h	i	j	k	l	m
Chiffré	d	e	f	g	h	i	j	k	l	m	n	o	p
Clair	n	o	p	q	r	s	t	u	v	w	x	y	z
Chiffré	q	r	s	t	u	v	w	x	y	z	a	b	c

   Le message chiffré est donc : ROBPSLDGHV.

2. Décoder le message suivant, chiffré par la méthode de César avec la clé 9 : JWWNN MNB VJCQNVJCRZDNB.

   Facilitons le déchiffrage en utilisant un tableau (décalage de 9).

Clair	a	b	c	d	e	f	g	h	i	j	k	l	m
Chiffré	j	k	l	m	n	o	p	q	r	s	t	u	v
Clair	n	o	p	q	r	s	t	u	v	w	x	y	z
Chiffré	w	x	y	z	a	b	c	d	e	f	g	h	i

   Le message en clair est : ANNEE DES MATHEMATIQUES.

3. Décoder les trois parties du texte suivant, chiffré par la méthode de César, dont la clé est à deviner :

Texte 1 : signé Alan Turing.

Chers amateurs de mathématiques,

Depuis ma naissance en *qmppi riyj girx hsydi*, la cryptographie me passionne. Le décodage est simpliste même si *Tcxleksvi ri ey wmbmiqi wmigpi ezerx Niwyw Glvmwx* l'aurait trouvé brillant.

Eper Xyvmrk

* Il s'agit d'un chiffre de César il faut donc en déterminer la clef. Le message est, nous le savons signe par Alan Turing. En considérant le nombre de lettres dans chaque mot cela signifie que ALAN et chiffré par EPER. En particulier A est chiffré par E.

La clef est donc 4.

* Facilitons le déchiffrage en utilisant un tableau (décalage de 4).

Clair	a	b	c	d	e	f	g	h	i	j	k	l	m
Chiffré	e	f	g	h	i	j	k	l	m	n	o	p	q

Clair	n	o	p	q	r	s	t	u	v	w	x	y	z
Chiffré	r	s	t	u	v	w	x	y	z	a	b	c	d

qmppi riyj girx hsydi
mille neuf cent douze
Tcxleksvi ri ey wmbmiqi wmigpi ezerx Niwyw Glvmwx
Pythagore ne au sixieme siecle avant Jesus Christ
Eper Xyvmrk
Alan Turing

Partie B.

Soient a et b deux nombres entiers. Le cryptage affine consiste à remplacer chaque lettre de l'alphabet par un nombre, en commençant par 0 pour la lettre A, 1 pour la lettre B... jusqu'à 25 pour la lettre Z, puis à remplacer le nombre initial x par le nombre y qui est le reste de la division euclidienne de $ax + b$ par 26. Le couple $(a; b)$ forme la clé du cryptage.

1. (a) Avec la clé $(a; b) = (22; 4)$, détailler les calculs pour la lettre B.

Si la lettre est B alors $x = 2$.
Donc : $ax + b = 22 \times 2 + 4 = 48$.

Puisque $48 > 25$ il faut faire la division euclidienne de 48 par 26 :

$$\begin{cases} 48 = 1 \times 26 + 22 \\ 0 \leqslant 22 < 26 \end{cases}$$

Donc $y = 22$.
Enfin la vingt-deuxième lettre de l'alphabet est W (en commençant la numérotation par 0).

Avec la clé $(a; b) = (22; 4)$, la lettre B est chiffré par W.

(b) Toujours avec la clé $(a; b) = (22; 4)$, coder les lettres D et Q.

*

$$\begin{aligned} \text{D} &\to x = 3 \\ &\to ax + b = 22 \times 3 + 4 = 70 \\ &\to y = 18 \quad \text{car } 70 = 2 \times 26 + 18 \\ &\to \text{S} \end{aligned}$$

*

$$\begin{aligned} \text{Q} &\to x = 16 \\ &\to ax + b = 22 \times 16 + 4 = 356 \\ &\to y = 18 \quad \text{car } 356 = 13 \times 26 + 18 \\ &\to \text{S} \end{aligned}$$

Les lettres D et Q sont codées par la lettre S.

(c) Quel problème pratique engendre l'utilisation de cette clé ?

Une même lettre chiffré peut correspondre à plusieurs lettres en clair.

Cette clé rend le message indéchiffrable.

2. On change de clé : on prend $(a; b) = (9; 4)$.
Dans l'algorithme ci-dessous, m % 26 désigne le reste de la division euclidienne de m par 26. par exemple, $28 \,\%\, 26 = 2$.

```
Entrer a
Entrer b
x ← 0
Tant que x < 26
        m ← ax +b
        y ← m % 26
        Afficher x, y
        x ← x + 1
Fin tant que
```

Cet algorithme permet de remplir le tableau de la question (a).

(a) Recopier sur votre copie le tableau ci-dessous et le compléter pour tout l'alphabet.

Lettre	A	B	C	D	E	F	G	H	I	...
Rang x	0	1	2	3	4	5	...	...	...	...
$m = ax + b$	4									
Rang y	4									
En crypté	E									

En programmant l'algorithme sur la calculatrice nous obtenons les valeurs du tableau.

Par exemple en Python :

```
a=int(input("a=?"))
b=int(input("b=?"))
x=0
while x<26:
    m=a*x+b
    y=m%26
    print("x=",x,"m=",m,"y=",y)
    x=x+1
```

Avec la Texas Instrument :

```
NORMAL FLOTT AUTO RÉEL DEGRÉ MP
ÉDIT MENU: [alpha] [f5]
PROGRAM:A
:Input "A=?",A
:Input "B=?",B
:0→X
:While X<26
:AX+B→M
:reste(M,26)→Y
:Disp X,M,Y
:Pause
:X+1→X
```

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
$m = ax + b$	4	13	22	31	40	49	58	67	76	85	94	103	112
Rang y	4	13	22	5	14	23	6	15	24	7	16	25	8
En crypté	E	N	W	F	O	X	G	P	Y	H	Q	Z	I

Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rang x	0	1	2	3	4	5	6	7	8	9	10	11	12
$m = ax + b$	121	130	139	148	157	166	175	184	193	202	211	220	229
Rang y	17	0	9	18	1	10	19	2	11	20	3	12	21
En crypté	R	A	J	S	B	K	T	C	L	U	D	M	V

(b) La clé $(9; 4)$ résout-elle le problème rencontré à la question 1.(c) ?

La clé $(9; 4)$ résout en effet le problème puisque chaque lettre cryptée ne correspond qu'à une seule lettre en clair.

(c) Décoder la partie du texte suivant, codé avec la clé $(a; b) = (9; 4)$.

Texte 2.

Le mot algorithme tire son origine de *Ez-Qpeuebyviy ro or kojt wort scetbo lyrgtk*, père de l'algèbre.

Grâce au tableau de la question 2.(a) :

Ez-Qpeuebyviy ro or kojt wort scetbo lyrgtk
Al-Khawarizmi ne en sept cent quatre vingts

3. Proposer un algorithme de décodage. Toute trace de recherche sera prise en compte.

```
Entrer a
Entrer b
Entrer z
x ← 0
Tant que x < 26
        m ← ax +b
        y ← m % 26
        Si y=z alors
                Afficher x
        x ← x + 1
Fin tant que
```

4. Quel est le principal défaut des deux systèmes de codage vus précédemment ?

   Pour le code César il n'y a que 25 clés possibles. Il est donc aisé de les tester toutes avec un outil informatique.

   Pour le chiffrage affine comme le message chiffré est obtenu avec des restes par division euclidienne par 26, il n'y a que 26 valeurs possible pour a et pour b (et encore nous avons vu que toutes ne fonctionnent pas à la question B.1.(b).). Là encore cela correspond pas à un grand nombre de possibilité à vérifier, du moins pour un ordinateur.

   Les deux précédents chiffrages résistent mal à une attaque par brute force (essayer toutes les possibilités).

Partie C.

On peut reprendre le chiffre de César de la partie A en changeant de clé pour chaque lettre. Ce chiffrement le chiffrement de Vigenère, introduit la notion de clé, qui peut se présenter sous forme d'un mot ou d'une phrase. On choisit par exemple le mot clé VIGENERE, ce qui donnera :

- la clé 21 (lettre V) pour la 1^{re} lettre du message à coder,
- la clé 8 (lettre I) pour la 2^{e} lettre,
- la clé 6 (lettre G) pour la 3^{e} lettre, etc...
- la clé 4 (lettre E) pour la 8^{e} lettre puis on recommence avec la clé 21 (lettre V) pour la 9^{e} lettre, etc.

1. Décoder avec cette clé la date de naissance de Blaise Vigenère.

Texte 3.

HQRPR GZRL KKRG ZZRBB-ZVBMJ

Crypté	H	Q	R	P	R	G	Z	R	L	K	K	R
Clef	V	I	G	E	N	E	R	E	V	I	G	E
Décalage	−21	−8	−6	−4	−13	−4	−17	−4	−21	−8	−6	−4
Clair	M	I	L	L	E	C	I	N	Q	C	E	N

Crypté	G	Z	Z	R	B	B	Z	V	B	M	J
Clef	N	E	R	E	V	I	G	E	N	E	R
Décalage	−13	−4	−17	−4	−21	−8	−6	−4	−13	−4	−17
Clair	T	V	I	N	G	T	T	R	O	I	S

HQRPR GZRL KKRG ZZRBB-ZVBMJ
MILLE CINQ CENT VINGT-TROIS.

2. Remplir la frise ci-dessous avec les noms des trois mathématiciens évoqués dans les textes précédents ainsi que leur année de naissance, parfois approximative.