Récréations Mathématiques

28 Janvier 2005

Le sujet est composé de deux parties indépendantes. Vous disposez de deux heures pour répondre à cinq questions de cours et un problème de votre choix.

Le Grand théorème de Fermat

Donner un énoncé précis du grand théorème de Fermat.

Théorie des jeux

Soit A et B deux ensembles finis non vides, et $f\colon A \times B \to \mathbf{R}$ une fonction. Quelle est la relation ($\leq$ ou $\geq$) entre les deux quantités

$$\min_{a\in A}\left\{\max_{b\in B} f(a,b)\right\} \qquad et \qquad \max_{b\in B}\left\{\min_{a\in A} f(a,b)\right\}.$$

Donner un exemple pour lequel l'inégalité est stricte.

Jeux de Nim

On considère le jeu suivant : deux individus sont faces à un tas de 15 allumettes et doivent retirer à tour de rôle, 1,2 ou 3 allumettes du tas. Celui qui retire les dernières allumettes a gagné.

1. Quel est le graphe correspondant à ce jeu ?;
2. Quelle est la fonction de Grundy de ce jeu ?
3. Expliquez comment gagner à ce jeu.

Autour du théorème de Thales

1. Théorème de Pythagorre Soit ABC un triangle rectangle en A. On note H le pied de la hauteur issue de A.
   En utisant des triangles semblables, montrer le théorème de Pythagorre.
2. Une implication du Théorème de Thalès Soit ABC un triangle quelconque, et E et F deux points respectivement de (AB) et (AC) tels que (EF) soit une droite paralèlle à (BC). En considérant successivement les triangles ABF, BCF, AEC et BCE, et en calculant leurs aires, montrer que $\frac{AF}{AC} = \frac{AE}{AB}$

Suite de Fibonacci

Définir la suite de Fibonacci et expliquer son lien avec le nombre d'or.

Le Jeu des erreurs

A quelle condition un code correcteur (tableau magique ou supermagique) peut-il corriger 1 erreur ? jusqu'à e erreurs (e entier non nul). Donner des exemples.

Modélisation Probabiliste

Un dé cubique et équilibré a 5 faces rouges et une face verte. Modéliser l'expérience aléatoire qui consiste en un lancer de ce dé (univers, probabilité).

Les Fractales

Soit F un sous-ensemble de $\mathbf{R}^n$ (avec $n = 1$, 2 ou 3). Donner la définition de la *dimension de boite* de F: $dim_B(F)$.

Les Nombres premiers

Montrer qu'il existe une infinité de nombres premiers.

Cryptographie

Citez deux algorithmes à clé secrètes et deux algorithmes clés publiques utilisés actuellement. Quelle est la taille de l'entier n pour une carte bancaire. Détaillez comment est obtenu la valeur VA inscrite sur la carte.

♠ ♡ ♢ ♣

Le Grand théorème de Fermat

Soit p un nombre premier. Démontrer le premier cas de l'exposant p de l'équation de Fermat c'est prouver l'implication :

$$x^p + y^p = z^p \Longrightarrow p \mid xyz$$

où x, y et z sont, bien entendu, supposés entiers.

(1) Soient a et b deux entiers. Établir la congruence :

$$(a+bp)^p \equiv a^p \mod p^2$$

en déduire que c^p prend au plus p valeurs modulo p^2 quand c décrit l'ensemble des entiers.

(2) Déterminer ces valeurs pour $p = 3$, en éduire le premier cas de Fermat pour l'exposant 3.

(3) Déterminer ces valeurs pour $p = 5$, en éduire le premier cas de Fermat pour l'exposant 5.

(4) Déterminer ces valeurs pour $p = 7$, Il y a une obstruction pour conclure. Laquelle ?

Théorie des jeux

- Donner tous les équilibres (en stratégies pures) du jeu suivant:

	b_1	b_2	b_3	b_4	b_5
a_1	1	2	3	2	1
a_2	0	3	-4	0	-1
a_3	-1	-2	2	7	$0,5$
a_4	1	$2,5$	6	3	1
a_5	0	5	4	1	-2

- On étudie le jeu suivant:

	b_1	b_2
a_1	-1	1
a_2	2	0

Ce jeu possède-t'il un équilibre? Sinon, déterminer un équilibre de Nash $(\overline{a}^*, \overline{b}^*)$ au sens des stratégies mixtes, et donner la valeur du jeu correspondante.

Jeux de Nim

Définition 1 *Un* graphe *est un couple $G = (X, U)$ où X est l'ensemble des* sommets *du graphe et U est une partie de $X \times X$ dont les éléments sont les* arcs *du graphe. Quand X est fini, le nombre de sommets est appelé* l'ordre du graphe*, sinon le graphe est dit* infini*. On définit l'ensemble des* successeurs *d'un sommet x par*

$$\Gamma(x) := \{y \in X,\ (x, y) \in U\}.$$

Définition 2 *Soit $G = (X, U)$ un graphe et S une partie de X. On dit que S est une partie* stable *de G si et seulement si elle vérifie :*

$$\forall x \in S, \quad \Gamma(x) \cap S = \varnothing \tag{1}$$

Définition 3 *Soit $G = (X, U)$ un graphe. Une partie A de X telle que*

$$\forall x \notin A, \quad \Gamma(x) \cap A \neq \varnothing \tag{2}$$

est appelée une partie absorbante *de G.*

Définition 4 *Soit $G = (X, U)$ un graphe. Une partie N de X à la fois stable et absorbante est appelée un* noyau *du graphe.*

Définition 5 *Soit $G = (X, U)$ un graphe sans boucles (i.e. $\forall x, (x, x) \notin U$). Une application $g : X \to \mathbf{N}$ est une* fonction de Grundy *si et seulement si*

$$\forall x \in X, \quad g(x) = \min\ \mathbf{N} \setminus g(\Gamma(x)) \tag{3}$$

1. Trouvez un graphe qui n'admet pas de noyau ;
2. Démontrez qu'un noyau est nécessairement une partie stable maximale et une partie absorbante minimale (au sens de l'inclusion des ensembles) ;
3. Démontrez que si un graphe admet une fonction de grundy g, alors les zéros de cette fonctions constituent un noyau du graphe.
4. On se donne un graphe $G = (X, U)$. On suppose que l'on a pu partitionner les sommets du graphes en k classes $X_1, X_2, \ldots, X_k$ construites de la manière suivante : la classe X_1 est l'ensemble des sommets du graphe qui n'ont pas de successeurs. On considère alors le nouveau graphe obtenu à partir de G en enlevant tous les sommets de X_1 et les arcs associés et on cherche à nouveau les sommets qui n'ont pas de successeurs pour X_2 et ainsi de suite jusqu'à épuisement de tous les sommets de X. Montrez que l'on peut déduire de cette partition une construction d'une fonction de Grundy pour ce graphe et ainsi un noyau.

Autour du théorème de Thales

Le but de ce petit problme est de prouver un résultat classique du triangle. On doit ce résultat à **Euler**.
Soit ABC un triangle. On notera D_1 la droite perpendiculaire à (BC) passant par A
(hauteur issue de A), D_2 la droite perpendiculaire à (AC) passant par B et D_3 celle perpendiculaire à (AB) passant par C.

1. Montrer, à l'aide du théorème de Pythagore, que l'ensemble des points qui sont à égale distance des points A et B est la droite perpendiculaire à (AB) passant par le milieu du segment $[AB]$.
   Cette droite est appelée <u>médiatrice de $[AB]$</u>.
   En déduire l'existence et la construction d'un unique cercle qui contienne les trois sommets du triangle.
   Ce cercle est appelé <u>le cercle circonscrit au triangle.</u>
   On note O son centre, et R son rayon.
   On notera Δ_1 la médiatrice de $[BC]$, Δ_2 celle de $[AC]$ et Δ_3 celle de $[AB]$.
2. Soit G le point défini par $\overrightarrow{AG}= \frac{1}{3}(\overrightarrow{AB} + \overrightarrow{AC})$.
   Montrer que $\forall M \in \mathcal{P}$, $3\ \overrightarrow{MG}=\overrightarrow{MA} + \overrightarrow{MB} + \overrightarrow{MC}$.
   En particulier, regarder ce qui se passe pour $M = G$.
   G est appelé <u>l'isobarycentre du triangle</u>.
3. Soit f l'homothétie de centre G, de rapport -2.
   (a) Déterminer par f les images par f des points A', B', C' et des droites Δ_1, Δ_2 et Δ_3.
   (b) En déduire que les hauteurs du triangle ABC sont concourrantes.
   On notera H leur point de concours : c'est <u>l'orthocentre du triangle ABC</u>.
   (c) En déduire que O, G et H sont alignés, et exprimer $\overrightarrow{GH}$ en fonction de $\overrightarrow{GO}$.

   La droite qui contient les points G, O et H est dite <u>droite d'Euler du triangle ABC</u> lorsqu'elle existe.
   Dans quel cas, cette droite n'existe pas ?
4. Soit h l'homothétie de centre G et de rapport $\frac{-1}{2}$.
   (a) Justifier que l'image de $\mathcal{C}$ est un cercle $\mathcal{C}'$ dont le centre O' est le milieu de $[OH]$.
   (b) Déterminer l'image du cercle $\mathcal{C}$ par l'homothétie h' de centre H, de rapport $\frac{1}{2}$.
   (c) Conclure que le cercle $\mathcal{C}'$ contient les milieux des côtés du triangle ABC, les pieds des hauteurs du triangle ABC et les milieux des segments $[HA]$, $[HB]$ et $[HC]$.

   Le cercle $\mathcal{C}'$ est appelé <u>cercle d'Euler du triangle ABC</u>.

Suite Fibonacci

On définit une suite par $Y_1 = Y_2 = 1$ et $Y_{n+2} = 2Y_{n+1} + Y_n$ pour $n \geq 1$.

- Calculer les six premiers termes de la suite.
- Montrer que la suite des Y_n tend vers l'infini.
- Montrer par récurrence que $Y_{n+1}^2 - Y_nY_{n+2} = 2(-1)^n$ pour tout $n \geq 1$.
- Soit $r_n = Y_n/Y_{n+1}$. Exprimer $r_{n+1} - r_n$ en fonction de Y_{n+1} et Y_{n+2}.
- Montrer que $\lim_{n\to\infty} r_n$ existe.
- Exprimer r_{n+1} en fonction de r_n et en déduire $r = \lim_{n\to\infty} r_n$.
- Développer r en fraction continue.

Le Jeu des erreurs

Construire un code correcteur (tableau magique) de longueur 6 et corrigeant 1 erreur (donner la liste de ses lments).

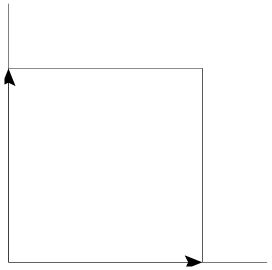
Modélisation Probabiliste

Caractérisation variationnelle de l'équiprobabilité.
Une roulette a n nombres numérotés 1,2 ...,n. Chaque nombre i a la probabilité $p_i \in]0, 1[$ de sortir. On fait tourner la roulette deux fois de suite en supposant que les deux expériences aléatoires successives sont indépendantes.
1) Calculer la probabilité que le numéro 1 sorte les deux fois.
2) Montrer que "les deux nombres sortis sont identiques" a une probabilité $S = \sum_{i=1}^{n} p_i^2$.
3) Montrer que S est minimale lorsque tous les p_i sont égaux à $\frac{1}{n}$. (On pourra introduire les nombres a_i définis par $p_i = \frac{1}{n} + a_i$.)

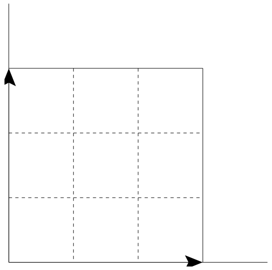
Les Fractales

le tapis de Sierpinski
On construit le tapis de Sierpinski par itération de la façon suivante: l'élément de base τ_0 est le carré unité (figure 1). On divise τ_0 en 9 carrés égaux (figure 2), et on retire le carré central: on obtient alors τ_1 (figure 3: la partie grisée

ne fait pas partie de τ_1, c'est cette partie qu'on a retirée).

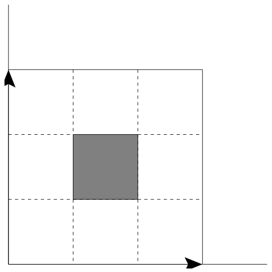


$figure1$

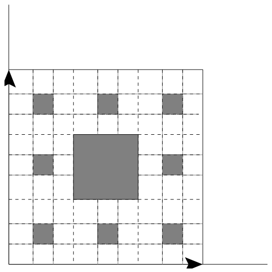


$figure2$

Il reste alors 8 carrés: on procède pour chacun comme pour τ_0 (on divise chacun en 9 et on retire le carré central): on obtient ainsi τ_2 (figure 4).



$figure3$



$figure4$

On construit ensuite τ_3, τ_4, ... de la même manière. Le tapis de Sierpinski τ est défini par

$$\tau \ := \ \bigcap_{i=0}^{\infty} \tau_i \ = \ \tau_0 \cap \tau_1 \cap \tau_2 \cap \dots$$

En supposant que la dimension de boite de τ (notée $dim_B(\tau)$) existe, la calculer.

Les Nombres Premiers

On s'intéresse à la primalité des nombres de la forme $a^m - 1$.

(1) On considère, pour tout entier $m > 0$, les nombres de la forme :

$$a^m - 1.$$

En remarquant que 1 est racine du polynôme $P(X) = X^m - 1$, factoriser le polynôme $P(X)$. En déduire que si $a^m - 1$ est premier alors $a = 2$.

(2) Montrer que si $2^m - 1$ est premier alors m est nécessairement premier (on montrera la contraposée : si m n'est pas premier alors $2^m - 1$ n'est pas premier).

(3) Les nombres $M_p = 2^p - 1$ avec p premier sont appelés nombres de Mersenne. Montrer que M_7 est premier.

(4) On dit qu'un nombre (entier) est parfait s'il est égal à la somme de ses diviseurs propres (1 est compté dans ses diviseurs propres mais pas le nombre lui-même). Par exemple, 6 est un nombre parfait car les diviseurs propres de sont $1, 2$ et 3 et $6 = 1 + 2 + 3$. Montrer que 28 est un nombre parfait.
Montrer que si M_p est un nombre de Mersenne premier alors l'entier

$$\frac{M_p(M_p+1)}{2} = 2^{p-1}(2^p - 1)$$

est un nombre parfait.

(5) On s'intéresse à la réciproque de la question 2) : si p est premier alors M_p est-il nécessairement premier ? On pourra utiliser le résultat numérique suivant :

$$3^{2046} \equiv 1013 \pmod{2047}.$$

Cryptographie

Il s'agit dans cet exercice de démontrer que pour tout entier a premier avec n, $a^{\phi(n)} \equiv 1$ modulo n où

$$\phi(n) = \{\text{card } a \in \mathbf{N}, 0 < a < n \mid \text{pgcd}(a, n) = 1\}$$

(1) Soient α et β deux entiers premiers avec n, montrez que $\alpha\beta$ est premier avec n.

(2) Notons $b_1, \dots, b_{\phi(n)}$ les $\phi(n)$ entiers strictement inférieurs à n qui sont premiers avec n. Déduisez de la question précédente que $\forall i = 1 \dots \phi(n)$, ab_i modulo n est premier avec n.

(3) En déduire que $\prod_{i=1}^{\phi(n)} ab_i \equiv \prod_{i=1}^{\phi(n)} b_i$ modulo n.

(4) Conclure (on rappelle que si x et y sont premiers entre eux alors il existe un entier $z < y$ t.q $xz \equiv 1$ modulo y.