STAGE OLYMPIQUE JUNIOR 2018

Cachan, 22 au 26 octobre 2018

Avant-propos

Le stage olympique junior de toussaint 2018 a été organisé à Cachan par l'association Animath.

Son objet a été de rassembler des élèves de seconde et de collège,
séléctionnés entre autres d'après leur participation à diverses compétitions
comme le concours Kangourou et l'Olympiade de Quatrième (concours René Merckhoffer)
et aux précédentes activités olympiques d'Animath,
notamment la coupe Animath de printemps du 6 juin 2018,
et de leur donner les bases nécessaires pour participer aux compétitions internationales.
Presque tous les stagiaires ont passé, le 3 octobre 2018,
la coupe Animath d'automne de la Préparation Olympique Française de Mathématiques,
mais celle-ci était trop tardive pour être pris en compte dans notre sélection.
Cela dit, certains de nos stagiaires
seront ainsi préparés à plusieurs compétitions internationales en 2019,
notamment les Olympiades Balkaniques Junior de Mathématiques
destinée précisément à des jeunes de leur âge

Nous tenons à remercier l'internat d'excellence de Cachan
pour son formidable accueil.

Les Animatheurs


Baptiste
SERRAILLE


Cécile
GACHET


Colin
DAVALO


François
LO JACOMO


Linda
GUTSCHE


Louise
GASSOT


Mathieu
BARRÉ


Matthieu
LEQUESNE


Paul
CAHEN


Raphaël
DUCATEZ


Razvan
BARBULESCU


Théo
LENOIR


Thomas
BUDZINSKI


Vincent
JUGÉ

Les élèves

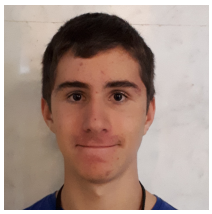

Agatha
BEFFY


Alexandre
BARBU

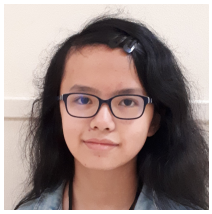

Alexandre
PAKIN


Amélie
TRIQUENEAUX


Amira
BERACHED


Brieux
MADELINE-DÉROU


Claire
BARDET


Clara
WU


Clementina
TIERNO


Dimitri
LEROU


Elie
VERHILLE


Elisa
ZHENG


Emilhan
DÜRRÜOGLU

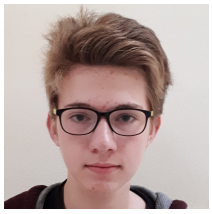

Emilie
LABONNE


Etienne
CONCHON-KERJAN


Félicité
COGNAT


François
NGUYEN VAN LONG


François
VOGEL


Galileo
GREY


Gaspard
DELABRE

Gwenc'Hlan
ARPHANT

Hannah
FAUCHEU

Ines
SOUA

Isidore
FONTAINE

Johanna
LEIBL

Justine
BOUYER

Leopold
FAUX- -RESNIER

Mano
ETILÉ

Manon
RAVARD

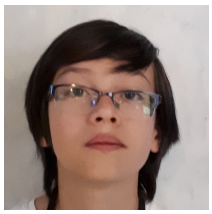
Marwan
PICAUD-CHEMRAKHI

Matthieu
VOGEL

Natacha
FRANSISCO

Nelly
CERF

Nicolas
BRIAND



Olivier
GRÉLY

Paul
GUICHON

Pénélope
NAZARET

Samy
MEZIANE

Timothée
TOULET

Zoé
LASSALE- -DERUELLE

Table des matières

I. Déroulement du stage

Pour le vingtième anniversaire d'Animath, c'est la dixième année que nous organisons ce stage olympique junior, et toujours - sauf la première année - au foyer de Cachan. En prévision des Olympiades Balkaniques Junior de Mathématiques, nous avons décidé de n'accepter que les élèves de quatrième, troisième ou seconde nés en 2004 ou après : parmi 65 candidatures vérifiant ces critères, après deux désistements, nous avons ainsi admis 40 stagiaires, dont 8 de seconde, 21 de troisième et 11 de quatrième (âge moyen 13 ans 9 mois), venus de 14 Académies : Paris (11 élèves), Versailles (9 élèves), Lyon (5 élèves), Rouen (3 élèves), Besançon, Bordeaux, Caen, Clermont-Ferrand, Créteil, Dijon, Grenoble, Nice, Poitiers et Rennes. Deux élèves venaient de l'étranger : Belgique et Pays Bas. Il y a encore trop de stagiaires des Académies de Paris et Versailles (50%), mais nous avons un nombre record de filles : 45% (2 de seconde, 9 de troisième et 7 de quatrième). La parité est à bout de bras...

Le premier jour, trois animateurs sont arrivés vers 8 h 15 pour tout préparer, et les stagiaires sont arrivés entre 9 h 55 et 12 h. Plusieurs familles ont été mises en contact afin de coordonner leurs voyages, et quatre élèves ont été accueillis gare de Lyon par Raphaël Ducatez, Linda Gutsche a réalisé très rapidement le trombinoscope. Après une rapide présentation du stage à 12 h, nous étions bien à l'heure pour le déjeuner à 12 h 30. L'après-midi devait permettre de constituer les deux groupes, les "avancés" qui avaient déjà manipulé les notions olympiques et les "débutants" qui venaient s'initier aux mathématiques de ocmpétitions, au moyen de questions écrites, de 14 h à 16 h, réunies ironiquement sous le nom "schibboleth". A 16 h, un premier goûter attendait les élèves, le dîner a été avancé à 18 h 30, suivi de la correction des exercices de la schibboleth. Hormis l'heure du dîner avancée d'une demi-heure, les horaires étaient ceux de l'an passé : petit déjeuner à 8 h, cours en parallèle de 9 h à 10 h 30 et de 11 h à 12 h 30, déjeuner à 12 h 30, cours de 14 h à 16 h et de 16 h 30 à 17 h 30 avec un goûter à 16 h, dîner à 18 h 30 suivi généralement d'une soirée à 20 h. Puis les stagiaires pouvaient encore jouer, mais à 23 h, extinction des feux. Je surveillais l'aile des garçons, secondé par Baptiste Serraille, Mathieu Barré et Thomas Budzinski, et Raphaël Ducatez surveillait l'aile des filles, secondé par Linda Gutsche, Colin Davalo et Cécile Gachet.

Mardi soir, Razvan Barbulescu a exposé toute l'histoire de la cryptographie, jusqu'au concours Al Kindi proposé précisément aux élèves de quatrième, troisième et seconde. Le lendemain, Matthieu Lequesne leur a présenté une grande diversité d'actions qui les concernent de l'association Animath. La plaquette d'Animath leur avait été distribuée à l'arrivée, avec le livret d'accueil. Des T-shirts avec le nouveau dessin de la POFM (Préparation Olympique Française de Mathématiques) ainsi que de nouveaux bics Animath leur ont été distribués. La dernière soirée, jeudi, était traditionnellement libre. Certains élèves se sont couchés plus tard que d'habitude, mais sans excès. La schibboleth du vendredi matin (9 h 30 à 12 h), avec des exercices différents pour les avancés et pour les débutants, portait sur les trois journées de

cours, où différents chapitres ont été abordés, mais avec une alternance moins systématique qu'aux stages précédents, a été corrigée vendredi après-midi, suivie par quelques formalités de départ... et la distribution du présent polycopié, pour une fin du stage prévue vers 16 h.

		Débutants	Avancés
Lundi	10h-12h	Arrivée et installation	
	12h-12h30	Présentation du stage	
	14h-16h	**Schibboleth des groupes**	
	20h	Correction de la schibboleth et répartition dans les groupes	
Mardi	Matin	géométrie (Linda Gutsche)	géométrie (Baptiste Serraille)
	Après-midi	inégalités + arithmétique (Raphaël Ducatez)	arithmétique + inégalités (Cécile Gachet)
	20h	**Les codes secrets, de l'antiquité à nos jours (Razvan Barbulescu)**	
Mercredi	Matin	géométrie et algèbre (Linda Gutsche)	géométrie + arithmétique (Baptiste Serraille)
	Après-midi	stratégies de base + arithmétique (Colin Davalo)	combinatoire (Raphaël Ducatez)
	20h	**Présentation d'Animath (Matthieu Lequesne)**	
Jeudi	Matin	stratégies de base (Vincent Jugé)	algèbre (Louise Gassot)
	Après-midi	pot-pourri d'exercices (Raphaël Ducatez)	combinatoire (Thomas Budzinski)
Vendredi	9h30-12h	**Schibboleth de fin de stage**	
	14h30	Correction de la schibboleth - clôture du stage	

Quelques liens utiles pour poursuivre le travail réalisé pendant ce stage :

— Le site d'Animath : `animath.fr`

— Le site de la POFM : `maths-olympiques.fr` et notamment :

— Les archives de problèmes (polycopiés etc...) : `maths-olympiques.fr/?page_id=4`

— Le site *MathLinks* : `mathlinks.ro`

— Le site *Art of Problem Solving* : `artofproblemsolving.com`

...

Le présent polycopié
ne contient pas l'intégralité des cours
et des exercices faits pendant le stage,
et beaucoup de solutions sont manquantes.
Le travail de rédaction des cours, exercices et solutions est long
et a déjà été fait maintes fois dans les précédents polycopiés.
La préparation olympique française de mathématiques (POFM)
s'efforce de trouver un autre moyen
de vous donner accès à toutes ces ressources accumulées au
cours de nos vingt années d'existence
sur son site `maths-olympiques.fr`,
autrement que par l'intermédiaire de polycopiés dont les
contenus peuvent être répétitifs

II. Première journée

1 Exercices d'échauffement

Exercice 1

Un triangle a des côtés de longueur 3, 4 et 5. Déterminer le rayon du cercle inscrit (cercle intérieur au triangle et tangent aux trois côtés).

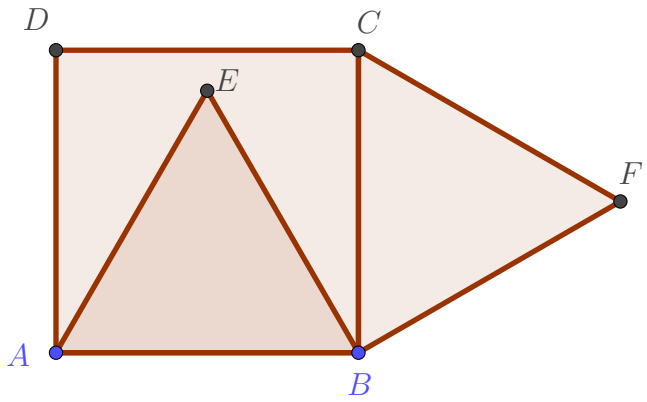
Exercice 2

Soient a, b, c, d quatre nombres réels positifs (par exemple : 0,8 ; 1,5 ; 1,1 ; 0,6) vérifiant : $a+b+c+d=4$.

Montrer que $ab+bc+cd+da \leq 4$.

Exercice 3

Sur la figure ci-dessous, $ABCD$ est un carré, ABE et BCF deux triangles équilatéraux. Montrer que les points D, E et F sont alignés.



Exercice 4

Déterminer tous les ensembles de six nombres entiers positifs $\{a\,;\,b\,;\,c\,;\,x\,;\,u\,;\,z\}$ tels que :

— $a \geq b \geq c$ et $x \geq y \geq z$

— $a+b+c=xyx$ et $x+y+z=abc$.

Solution de l'exercice 1

Si l'on appelle I le centre du cercle inscrit, et r le rayon du cercle inscrit, comme r est la hauteur de chacun des triangles IAB, IBC et ICA, l'aire de ces triangles vaut : $\frac{1}{2}r \times AB$, $\frac{1}{2}r \times BC$, $\frac{1}{2}r \times CA$, donc leur somme vaut rp en appelant p le demi-périmètre $\frac{1}{2}(AB+BC+CA)$.

Or la somme de ces trois aires est précisément l'aire S du triangle ABC, quel que soit le point I à l'intérieur du triangle, et en vertu du théorème de Pythagore, comme $3^2 + 4^2 = 5^2$, ce triangle est rectangle. Son aire vaut $S = \frac{1}{2}(3 \times 4) = 6$, son demi-périmètre, $p = \frac{1}{2}(3+4+5) = 6$, donc le rayon de son cercle inscrit vaut : $r = \dfrac{S}{p} = 1$.

Solution de l'exercice 2

$ab + bc + cd + da = (a + c)(b + d)$, or $(a + c) + (b + d) = 4$ par hypothèse. Il suffit donc de démontrer que si deux nombres réels $x = a + c$ et $y = b + d$ ont pour somme 4, leur produit vaut au plus 4. Or $(x - y)^2 = (x + y)^2 - 4xy = 16 - 4xy \geq 0$, ce qui entraîne bien que $xy \leq 4$. Avec les quatre nombres donnés en exemple, $ab + bc + cd + da = 3,99$.

Solution de l'exercice 3

Les trois angles du triangle ABE valent $60°$, tout comme les trois angles du triangle BCF. Donc $\widehat{DAE} = 30°$. Or le triangle DAE est isocèle, ses angles à la base sont donc égaux à $\dfrac{180° - 30°}{2} = 75°$. D'où $\widehat{CDE} = 15°$. De la même manière, le triangle CDF est isocèle, d'angles $\widehat{DCF} = 90° + 60° = 150°$, d'où $\widehat{CDF} = \dfrac{180° - 150°}{2} = 15° = \widehat{CDE}$. Cette égalité d'angles entraîne que les droites (DE) et (DF) sont confondues, donc que $D,\ E$ et F sont alignés.

Solution de l'exercice 4

Parmi les deux produits $abc = x+y+z$ et $xyz = a+b+c$, l'un est inférieur ou égal à l'autre, et on peut supposer (quitte à échanger $\{a; b; c\}$ et $\{x; y; z\}$) que $abc \leq xyx$, donc $abc \leq a+b+c$. Or lorsque $b \geq c \geq 2$, $bc \geq b + c \geq 4$, vu que $bc - (b + c) = (b - 1)(c - 1) - 1 \geq 0$. Et comme $a \geq 2$ et $bc \geq 4$, $a(bc) - (a + bc) = (a - 1)(bc - 1) - 1 \geq 2$, donc $a(bc) > a + bc \geq a + b + c$, ce qui est contraire à l'hypothèse. Donc on a nécessairement $c = 1$.

Dès lors, la condition $abc \leq a + b + c$ s'écrit : $ab \leq a + b + 1$, soit $(a - 1)(b - 1) \leq 2$. Comme $a \geq b$, de deux choses l'une :

— soit $b = 1$, et a peut être quelconque,

— soit $b = 2$, et $a \leq 3$, donc $(a = 2)$ ou $(a = 3)$.

Dans le premier cas, $xyz = a + 2$ et $x + y + z = a$.

1. Si $z = 1$, $xy = x + y + 3$, donc $(x - 1)(y - 1) = 4$. Comme $x \geq y$,
   — soit $x = 5$, $y = 2$ et $z = 1$, $a = 8$, $b = c = 1$: c'est effectivement une première solution,
   — soit $x = y = 3$, $z = 1$, $a = 7$, $b = c = 1$: c'est une seconde solution.
2. Si $z \geq 2$, $yz \geq 4$. Donc $4x \leq a + 2$ et $3x \geq x + y + z \geq a$. Cette toute dernière inégalité équivaut à $4x \geq \dfrac{4}{3}a$. Si on la rapproche de la première, $\dfrac{4}{3}a \leq a + 2$, soit $a \leq 6$ et $xyz \leq 8$. Comme $x \geq y \geq z \geq 2$, la seule possibilité est $x = y = z = 2$, $a = 6$ et $b = c = 1$.

Dans le second cas,

1. soit $a = b = 2$, $c = 1$, $xyz = 5$ n'est possible que si $x = 5$, $y = z = 1$, qui n'est pas solution car alors $x + y + z = 7$ n'est pas égal à $abc = 4$,
2. soit $a = 3$, $b = 2$ et $c = 1$, auquel cas $xyz = 6$, d'où

— soit $x = 6$, $y = z = 1$, ce qui n'est pas possible car alors $x + y + z = 8$ n'est pas égal à $abc = 6$,

— soit $x = 3$, $y = 2$ et $z = 1$, ce qui fournit une quatrième solution.

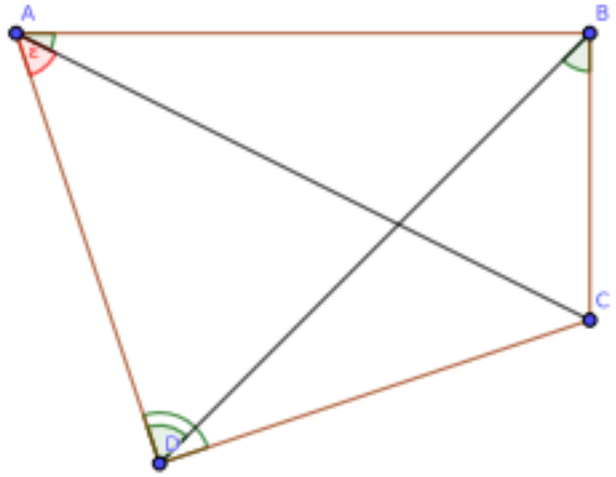
Le problème posé admet donc quatre solutions pour lesquelles $abc \leq xyz$:
$\{8; 1; 1; 5, 2; 1\}$ - $\{7; 1; 1; 3; 3; 1\}$ - $\{6; 1; 1; 2; 2; 2\}$ - $\{3; 2; 1; 3; 2; 1\}$
et donc évidemment 7 solutions si l'on n'impose pas $abc \leq xyz$, ce qui rajouterait :
$\{2; 2; 2; 6, 1; 1\}$ - $\{3; 3; 1; 7; 1; 1\}$ - $\{5; 2; 1; 8; 1; 1\}$.

2 Schibboleth des groupes

Géométrie

Question. *Connaissez vous les relations des angles inscrits et de l'angle au centre ? Si oui les énoncer.*

Exercice 1. Sur la figure suivante, on $\widehat{DBC} = 40°$, $\widehat{CAB} = 20°$, $\widehat{CDA} = 50°$, $\widehat{BDA} = 30°$. Trouvez la valeur de $\widehat{CAD}$.



Algèbre

Question. *Connaissez vous l'inégalité du réordonnement ? Si oui l'énoncer.*

Exercice 2. Démontrez que

$$38,7 \times 2,9 + 38 \times 3 + 38,9 \times 1,9 + 40 \times 1 + 10 \times 3,1 < 38 \times 1,9 + 40 \times 3 + 10 \times 2,9 + 38 \times 3,1 + 38,7 \times 1$$

Question. *Connaissez l'inégalité arithmétique et géométrique ? l'inégalité géométrique et harmonique ? Si oui les énoncer.*

Combinatoire

Question. *Connaissez vous les coefficients binomiaux ?*

Exercice 3. Montrez que

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Question. Connaissez vous le raisonnement par récurrence ?

Exercice 4. Montrez que

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$$

Arithmétique

Question. *Connaissez vous les modulos ? Si oui que vaut le reste de la division de* 10^6 *par* 11 *?*

Exercice 5. Trouver les entiers n tels que $n-1$ divise n^2+2

Problèmes pour vous occuper si vous avez le temps.

Exercice. (Bonus 1) : Soit n un entier naturel. Montrer que $\sqrt{n}$ est soit un entier naturel, soit un irrationnel (c'est à dire, qu'il n'existe pas p, q des entiers tel que $\sqrt{n} = \frac{p}{q}$).

Exercice. (Bonus 2) : Trois pays ont chacun envoyé n mathématiciens à une conférence. Chaque mathématicien a des échanges avec $n+1$ des mathématiciens qui ne sont pas de son pays. Prouver qu'il existe trois mathématiciens qui ont deux à deux eu des échanges.

III. Débutants

1 mardi 23 matin : Linda Gutsche

Les exercices

Tous les théorèmes du cours ont été vu sous forme d'exercices. Pour revoir certains aspects en profondeur ou en apprendre plus, je vous conseille d'étudier l'excellent polycopié de Cécile Gachet, disponible sur le site de la préparation : http://maths-olympiques.fr/wp-content/uploads/2017/09/geom_base.pdf

Exercice 1 : Centre du cercle circonscrit
Montrez que les médiatrices d'un triangle sont concourantes et que ce point de concurrence est le centre du cercle circonscrit au triangle.

Exercice 2 : Théorème de l'angle au centre
Soit Γ un cercle de centre O et A, B et C trois points sur ce cercle. Alors $\widehat{BOC} = 2 * \widehat{BAC}$

Exercice 3 : Théorème de l'angle inscrit version 1
Soit Γ un cercle et A, B, C et D dans cet ordre quatre points sur ce cercle. Alors $\widehat{ABD} = \widehat{ACD}$
Remarque : La réciproque est également vraie : si il y a égalité des angles, alors les points sont cocycliques.

Exercice 4 : Théorème de l'angle inscrit version 2
Soit Γ un cercle et A, B, C et D dans cet ordre quatre points sur ce cercle. Alors $\widehat{ADC} = 180 - \widehat{ABC}$
Remarque : Comme pour l'autre version, la réciproque est également vraie : si il y a égalité des angles, alors les points sont cocycliques.

Exercice 5 : Théorème de la tangente
Soit Γ un cercle et A, B, C et trois points sur ce cercle. Soit t la tangente à Γ en C (la tangente est une droite qui coupe le cercle en un unique point, et a la proriété d'être perpendiculaire au rayon). Alors l'angle que t forme avec BC est de mesure égale á celle de $\widehat{CAB}$
Remarque : Comme pour les théorèmes des angles inscrits, la réciroque est également vraie : si il y a égalité des angles, alors t est tangente au cercle circonscrit à ABC en C.

Exercice 6 :
Nous avons vu les solutions pour quatre différentes versions de cet exercices (qui dépendent

d'où se situent les points sur les cercles)
Soit Γ_1 et Γ_2 deux cercles qui s'intersectent en B et E. Soit A et D deux points de Γ_1 tels que (AB) et (DE) recoupent Γ_2 en respectivement deux points C et F. Montrer que (AD) parallèle à (CF).

2 mardi 23 après-midi : Raphaël Ducatez

1 Introduction aux modulos

Remarque Les exercices et les exemples peuvent être un peu différent de ceux présentés durant le cours.

Exemple 1 Le chiffre des unités de $(211 \times 13 \times 92)$ est 6. En effet il suffit de ne garder que le chiffre des unités de chaque terme et la multiplication donne $1 \times 3 \times 2 = 6$.

Exemple 2 Si a est pair, b est impair, c est impair et d est pair alors on peut affirmer que

$$(a+b) \times c + d$$

est impair. Remarquer que pour cela pas besoin de connaître explicitement a, b, c, d.

La division euclidienne

C'est la division que vous avez déjà vu lorsque vous êtiez plus jeune. Par exemple, si vous avez 25 billes et des sacs qui peuvent contenir 7 billes, vous pouvez remplir 3 sacs et il reste alors 4 billes.

Voici ici la définition formelle

Définition La division euclidienne :

Soit n un entier. Soit p un entier. Alors il existe des uniques entiers q et r tel que

$$p = q \times n + r$$

avec $0 \leq r < n$. Et on appelle r le reste de la division (euclidienne) de p par n. Dans notre exemple, on a $p = 24$, $n = 7$, $q = 3$ et $r = 4$ (remarquer que l'on a bien $r < n$, sinon on aurait pu faire un sac supplémentaire.)

Démonstration Existence : On choisit q le plus grand entier tel que $p \geq q \times n$. On pose alors

$$r = p - q \times n.$$

Il faut maintenant vérifier que $0 \leq r < n$. Puisque $p \geq q \times n$ alors on a bien $r \geq 0$. Imaginons que $r \geq n$ mais alors $p - q \times n \geq n$ et donc $p - q \times n + q \times n \geq n + q \times n$ (on ajoute des deux coté de l'inégalité la même chose) et $p \geq (q+1) \times n$. Mais on avait dit que l'on choisissait q le plus grand entier tel que $p \geq q \times n$. Ce n'est donc pas possible. La conclusion est que $r \leq n$ comme vu.

Unicité : on a trouvé un r et un q mais est-ce les seuls ? Supposons qu'il en existe deux

$$p = q_1 \times n + r_1 \qquad \text{et} \qquad p = q_2 \times n + r_2$$

et on peut supposer $q_1 \geq q_2$ (sinon on échange q_1 avec q_2 et r_1 avec r_2). On a

$$q_1 \times n + r_1 = q_2 \times n + r_2$$

et donc en retirant de chaque coté

$$q_1 \times n + r_1 - q_2 \times n = q_2 \times n + r_2 - q_2 \times n$$

pour obtenir

$$(q_1 - q_2) \times n + r_1 = r_2$$

Imaginons maintenant que $q_1 - q_2 \geq 1$. Alors $(q_1 - q_2) \times n \geq n$ et donc que $r_2 \geq n$ mais ça ce n'est pas possible car cela contredirait la définition. Conclusion, on ne peut pas avoir $q_1 - q_2 \geq 1$ et puisque $q_1 \geq q_2$ on a forcement $q_1 = q_2$. Et alors $(q_1 - q_2) \times n = 0$ et donc $r_1 = r_2$.
Exercice 1 Quel est le reste de la division euclidienne de 11 par 3 ? de 23 par 8 ?

Les modulos

Définition 1. (Modulo) Soit un entier n. Soient a, b des entiers. On dit que

$$a \equiv b[n]$$

(cela se lit « a est égale à b modulo n ») si le reste de la division de a par n est égale au reste de la division de b par n.

Exemple. On a
— $7 \equiv 4[3]$, en effet $7 = 3 \times 2 + 1$ et $4 = 3 \times 1 + 1$, donc 7 et 4 ont le même reste égale à 1.
— $11 \equiv 18[7]$ car $11 = 7 \times 1 + 4$ et $18 = 7 \times 2 + 4$.

On peut donner une autre définition des modulos qui est bien sur equivalente celle ci dessus.

Définition
(modulo)
Soit n un entier et soient a, b des entiers. On dit que

$$a \equiv b[n]$$

si n divise $b-a$. C'est aussi équivalent à dire qu'il existe k un entier tel que $b = a+k\times n$. Dans nos exemple précédent : $7 \equiv 4[3]$ car $7 = 4 + 3 \times 1$. De même $11 \equiv 18[7]$ car $11 = 18 + 7 \times (-1)$
Exercice 2 dites pour les affirmations suivant si elles sont vrai ou fausses.
— $8 \equiv 2[3]$
— $12 \equiv 2[4]$
— $23 \equiv 103[10]$
— $7 \equiv -2[9]$

Remarque 2. Pour le cas modulo 2, le reste de la division est soit 0 soit 1. Cela correspond à la parité : $a \equiv 0[2]$ si a est pair et $a \equiv 1[2]$ si a est impair.

Pour le cas modulo 10, le reste de la division est le chiffre des unités. On peut alors dire que $a = b[10]$ si et seulement si le chiffre des unités de a est égale au chiffre des unités de b (par exemple $17 \equiv 127[10]$).

Remarque 3. On a que n divise a si et seulement si $a \equiv 0[n]$.

Proposition 4. La somme des modulos
Soit n un entier. Soit a, b, c et d des entiers tel que

$$a \equiv b[n] \qquad \text{et} \qquad c \equiv d[n]$$

alors

$$a + c \equiv b + d[n].$$

Exemple
$13 \equiv 7[6]$ (car $13 = 7 + 6 \times 1$ et $2 \equiv 26[6]$ car $26 = 2 + 6 \times 4$) alors

$$(13 + 2) \equiv (7 + 26)[6].$$

On a en effet $15 \equiv 33[6]$ car $33 = 15 + 3 \times 6$.

Démonstration. Soit n et a, b, c, d comme dans l'énoncé. Alors il existe un entier k tel que $b = a + k \times n$. De même, il existe k' tel que $d = c + k' \times n$. On a donc

$$b + d = a + k \times n + c + k' \times n$$

et donc

$$b + d = (a + c) + (k + k') \times n$$

conclusion

$$(a + c) \equiv (b + d)[n].$$

□

Proposition 5. la multiplication des modulos
Soit n un entier. Soit a, b, c et d des entiers tel que

$$a \equiv b[n] \qquad \text{et} \qquad c \equiv d[n]$$

alors

$$a \times c \equiv b \times d[n].$$

Exemple
Exemple $8 = 2[3]$ et $4 \equiv 1[3]$ alors $8 \times 4 \equiv 1 \times 2[3]$. Et en effet $32 = 2 + 3 \times 10$.

Démonstration. Soit n et a, b, c, d comme dans l'énoncé. Alors il existe un entier k tel que $b = a + k \times n$. De même, il existe k' tel que $d = c + k' \times n$. On a donc

$$b \times d = (a + k \times n) \times (c + k' \times n)$$

par distributivité, on obtient

$$b \times d = a \times c + a \times k' \times n + k \times n \times c + k \times n \times k' \times n$$

et on regroupe les termes en n :

$$b \times d = a \times c + (a \times k' + k \times c + k \times n \times k') \times n$$

conclusion

$$(a \times c) \equiv (b \times d)[n].$$

□

Exercice 3 Dites si les affirmations suivantes sont vrai ou fausses.

— $302 \times 8 = 11[3]$

— $19 - (14 \times 7) \equiv 28 \times 3[2]$

— $13 \times 218 \equiv -2[10]$

— $35 + 41 \times 17 \equiv 22 - 6[5]$

Proposition 6. Puissance sur les modulos

Soit n un entier. Soit a et b des entiers tel que

$$a \equiv b[n]$$

alors

$$a^2 \equiv b^2[n],$$
$$a^3 \equiv b^3[n]$$

et pour tout entier i

$$a^i \equiv b^i[n]$$

où $a^i = a \times a \times \cdots \times a$ multiplié i fois.

Exemple

$8 \equiv 2[3]$ et donc $8^2 \equiv 2^2[3]$ en effet on peut vérifier que $64 = 21 \times 3 + 1$ et $4 = 1 \times 3 + 1$.
$11 \equiv 2[9]$ et donc $11^3 \equiv 2^3[9]$.

Démonstration. On utilise la propriété précédente avec $a \equiv b[n]$ et on choisi également a pour c et b pour d. Alors

$$a \times a \equiv b \times b[n]$$

Maintenant, on sait que $a \equiv b[n]$ et $a \times a \equiv b \times b[n]$ alors en avec la propriété précédente

$$a \times a \times a \equiv b \times b \times b[n].$$

On peut répéter la même démarche i et on obtient

$$a \times \cdots \times a = b \times \cdots \times b[n]$$

où on a multiplié de chaque coté i fois. □

Exercice 4 Compléter les $?$ avec des nombres entre 0 et 4 ou entre 0 et 7.

— $21^3 \equiv ?[4]$

— $6^8 \equiv ?[7]$

— $2^{10} \equiv ?[7]$

Correction : $21 \equiv 1[4]$ car $21 = 4 \times 5 + 1$. Donc $21^3 \equiv 1^3[4]$, conclusion $21^3 \equiv 1[4]$.
$6^8 = -1[7]$ car $6 = -1 + 1 \times 7$. Donc $6^8 = (-1)^8[7]$ et donc $6^8 \equiv 1[7]$
Calculons $2^2 \equiv 4[7]$, $2^3 \equiv 8[7]$ et donc $2^3 \equiv 1[7]$. Alors on a

$$2 \times 2^3 \times 2^3 \times 2^3 \equiv 2 \times 1 \times 1 \times 1[7]$$

et on peut conclure $2^{10} \equiv 2[7]$.

2 Critère de divisibilité :

Vous avez tous appris il y a longtemps que pour vérifier si un nombre est divisible par 9 (ou par 3), on fait la somme de ses chiffres et on regarde si cette somme est divisible par 9 (ou par 3).

Un peu moins connu, pour savoir si un nombre est divisible par 11, il suffit de verifier si la somme alterné de ses chiffres est divisible par 11.

Par exemple 981 est divisible par 9 car $9+8+1=18$ est bien divisible par 9 mais pas par 11 car $9-8+1=2$ n'est pas divisible par 11. Autre exemple : 7854 et divisible par 11 car $-7+8-5+4=0$ est bien divisible par 11.

On va montrer cette proposition grâce aux modulos.

Proposition 7. Soit p un entier que l'on peut écrire en chiffre $a_k \cdots a_2 a_1 a_0$ (a_0 est le chiffre des unités, a_1 est le chiffre des dizaines, a_2 des centaines, etc... dans notre exemple avec 981, $a_0 = 1$, $a_2 = 8$ et $a_3 = 9$)

Alors 9 divise p si et seulement si 9 divise $a_k + \cdots + a_1 + a_0$ la somme de ses chiffres.

De même, 3 divise p si et seulement si 3 divise $a_k + \cdots + a_1 + a_0$ la somme de ses chiffres.

Démonstration. (on le fait pour 9, pour 3 c'est la même démonstration) :

On a que $10 \equiv 1[9]$ d'après la propriété précédente on a que

$$100 \equiv 1[9]$$

$$1000 \equiv 1[9]$$

pour tout i ,

$$10^i \equiv 1[9]$$

On écrit $p = 10^k \times a_k \cdots + 100 \times a_2 + 10 \times a_1 + 1 \times a_0$ alors

$$p \equiv 10^k \times a_k \cdots + 100 \times a_2 + 10 \times a_1 + 1 \times a_0[9]$$

et donc

$$p \equiv 1 \times a_k \cdots + 1 \times a_2 + 1 \times a_1 + 1 \times a_0[9]$$

$$p \equiv a_k \cdots + a_2 + a_1 + a_0[9]$$

Conclusion p est égale à la somme de ses chiffres modulo 9. En particulier, $p \equiv 0[9]$ si et seulement si $a_k + \cdots + a_1 + a_0 \equiv 0[9]$ et donc p est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9. □

Proposition 8. Soit p un entier que l'on peut écrire en chiffre $a_k \cdots a_2 a_1 a_0$

Alors 11 divise p si et seulement si 11 divise $(-1)^k \times a_k + \cdots - a_3 + a_2 - a_1 + a_0$ la somme alternée de ses chiffres.

Démonstration. On a que $10 \equiv -1[11]$ d'après la propriété précédente on a que

$$100 \equiv 1[11]$$

$$1000 \equiv -1[11]$$

pour tout i ,

$$10^i \equiv (-1)^i[11]$$

c'est à dire $10^i \equiv -1[11]$ si i est impair et $10^i \equiv 1[11]$ si i est pair.

On écrit $p = 10^k \times a_k \cdots + 100 \times a_2 + 10 \times a_1 + 1 \times a_0$ alors

$$p \equiv 10^k \times a_k \cdots + 100 \times a_2 + 10 \times a_1 + 1 \times a_0[9]$$

et donc

$$p \equiv (-1)^k \times a_k \cdots + 1 \times a_2 + -1 \times a_1 + 1 \times a_0[9]$$

$$p \equiv a_k \cdots + a_2 - a_1 + a_0[9]$$

Conclusion p est égale à la somme alterné de ses chiffres modulo 11. En particulier, $p \equiv 0[11]$ si et seulement si $(-1)^k \times a_k + \cdots - a_1 + a_0 \equiv 0[9]$ et donc p est divisible par 11 si et seulement si la somme de ses chiffres est divisible par 11. □

Exercice 1 193116 est il divisible par 3? par 9? par 11 ? par 33 ? par 99 ?

Exercice 2 Que vaut le reste de la division de 705432^{50} par 11 ?

3 mercredi 24 matin : Linda Gutsche

Les exercices

Exercice 1 : Orthocentre
Montrez que les hauteurs d'un triangle sont concourantes. Ce point est appelé orthocentre de ABC.

Exercice 2 : Centre du cercle inscrit
Montrez que les bissectrices d'un triangle sont concourantes et que ce point de concurrence est le centre du cercle inscrit au triangle.

Exercice 3 : Théorème de Miquel
Soit ABC un triangle, et P, Q et R trois points quelconques sur respectivement $[BC]$, $[CA]$ et $[AB]$. Montrer que les cercles circonscrits à AQR, BRP et CPQ sont concourants.

Exercice 4 :
Soit ABC un triangle et H_A, H_B et H_C respectivement les pieds des hauteurs issues de A, B et C dans ABC. Montrer que H, l'orthocentre de ABC, est le centre du cercle inscrit à $H_AH_BH_C$

4 mercredi 24 après-midi : Colin Davalo

L'objectif de ce cours est de découvrir les stratégies de base pour la résolution de problèmes d'olympiades, et de découvrir l'arithmétique des nombres premiers. Pour un cours plus détaillé, n'hésitez pas à consulter les cours de la pofm disponibles sur le site maths-olympiques.fr, traitant de stratégies de base, et d'arithmétique.

Le principe des tiroirs

Le principe des tiroirs part d'une idée intuitive : si on a $n+1$ chaussettes à mettre dans n tiroirs, alors deux chaussettes seront dans le même tiroir. Cependant cette idée simple peut s'appliquer pour résoudre des problèmes plus difficiles.

Exercice 1 Seize étudiants passent une épreuve avec trois exercices. Chaque étudiant résout un exercice. Démontrer qu'au moins 6 étudiants ont résolu le même exercice.

Solution de l'exercice 1 On a 16 étudiants à ranger dans 3 catégories, ainsi si on suppose par l'absurde qu'au plus 5 étudiants ont résolu chaque exercice, alors on aurait que 15 étudiant : ce qui est une contradiction.

Exercice 2 Les points du plan sont coloriés de telle sorte que chaque point soit rouge ou bleu. Montrer que pour tout réel $x > 0$ il existe une couleur telle qu'on puisse trouver deux points de cette couleur distants de x.

Solution de l'exercice 2

On considère un triangle équilatéral de côté x. Il existe alors deux sommets de ce triangle qui conviennent.

Exercice 3 * On place 51 points sur un carré de côté 1. Montrer qu'on peut en trouver au moins 3 à l'intérieur d'un cercle de rayon $\frac{1}{7}$ (ce cercle peut déborder sur les cotés du carré).

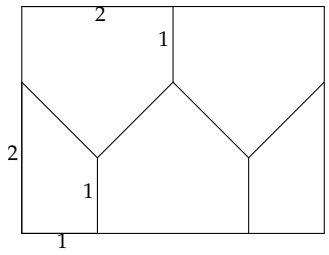
Solution de l'exercice 3 Pour appliquer le principe des tiroirs, il faut moins de $\frac{51}{2}$ tiroirs, soit au plus 25. Couvrir un carré avec 25 cercles est moins facile que le couvrir avec 25 carrés, de côté $\frac{1}{5}$. Mais la diagonale d'un tel carré mesure $\frac{\sqrt{2}}{5} < \frac{2}{7}$, de sorte que chacun de ces carrés est inclus dans un cercle de rayon $\frac{1}{7}$. Les trois points qui se trouvent à l'intérieur d'un même carré se trouvent a fortiori à l'intérieur d'un même cercle.

Exercice 4 On place 6 points à l'intérieur d'un rectangle de dimension 4×3. Montrer qu'on peut en trouver deux dont la distance est inférieure ou égale à $\sqrt{5}$.

Solution de l'exercice 4 Si l'on plaçait 7 points, le problème serait facile, il suffirait de diviser le rectangle en six rectangles 2×1. Mais on n'a que 6 points, il faut donc trouver un autre découpage astucieux. La figure nous montre quel découpage choisir. A l'intérieur d'un de ces six polygones, il y a deux points au moins, et leur distance est nécessairement inférieure à la plus grande diagonale du polygone, donc à $\sqrt{5}$.

Exercice 5 Dans un groupe de 6 personnes, montrer qu'on peut en trouver trois qui se connaissent, ou trois qui ne se connaissent pas, sachant que la relation de connaissance est réciproque.

Solution de l'exercice 5 On considère une personne A, soit elle connait trois personnes soit elle n'est pas connue de trois personnes par principe des tiroirs. Si elles en connait trois ,on considère alors B, C, D ces trois personnes. alors soit ces trois la ne se connaissent pas, ou bien



deux d'entre elles se connaissent et alors elles se connaissent avec A. L'autre cas se traite de même.

Exercice 6 Soit a un nombre réel positif. Montrer qu'il y a au moins un nombre dans$\{a, 2a, \cdots, (n-1)a\}$ qui est à distance au plus $\frac{1}{n}$ d'un nombre entier.

Solution de l'exercice 6 On regarde les restes de ces entiers modulo 1. Avec 0 et 1 cela fait $n+1$ éléments de $[0;1]$, donc par le principe des tiroirs on peut en trouver deux dans un même intervalle de la forme $[\frac{k}{n}; \frac{k+1}{n}]$ avec k un entier. Ainsi soit on a directement q'un élément de $\{a, 2a, \cdots, (n-1)a\}$ est proche d'un entier car sa partie fractionnaire est proche de 0 ou 1, ou bien on trouve que $|la - ma| < \frac{1}{n}$. Donc $(l-m)a$ est à distance au plus $\frac{1}{n}$ d'un entier.

Nombres premiers

Définition 9. On dit qu'un entier a divise b si il existe un entier c tel que $ac = b$. On dit aussi dans ce cas que b est divisible par a, ou encore que a est un diviseur de b. On le note $a|b$.

Tout entier strictement positif n est divisible par 1, et par n. On dit qu'un nombre $p > 1$ est premier si ses seuls diviseurs sont 1 et p.

Théorème 10 (Lemme de Gauss)**.** Soit p un nombre **premier**, et a, b deux entiers. Si p divise ab, alors p divise a ou p divise b.

Ce résultat n'est pas toujours vrai si p n'est pas premier : 6 divise 2×3 mais 6 ne divise ni 2 ni 3.

Théorème 11. Tout entier strictement positif n peut s'écrire sous la forme :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_k^{\alpha_k}$$

Cette écriture s'appelle la décomposition en facteurs premiers de n. De plus cette écriture est unique à permutation des p_i près, c'est à dire en particulier qu'elle est unique si on impose $p_1 < p_2 < \cdots < p_k$.

Exercice 7 Décomposer en facteurs premiers les entiers 2,4,6,9,17,72.

Solution de l'exercice 7

$2 = 2^1$, $4 = 2^2$, $6 = 2 \times 3$, $9 = 3^2$, $17 = 17^1$, $72 = 2^3 \times 3^2$. Pour décomposer un entier en facteurs premiers n on cherche un diviseur de n premier p (par exemple le plus petit diviseur strict de n), et on décompose $\frac{n}{p}$ en facteurs premiers.

Définition 12. Pour un entier strictement positif n, et un nombre premier p, on note $\nu_p(n)$ le plus grand entier k tel que p^k divise n. C'est également l'exposant de p dans la décomposition en facteurs premiers.

Exercice 8 Que vaut $\nu_3(18^{100})$?

Solution de l'exercice 8 L'entier $18^{100} = 2^100 \times 3^{200}$, est divisible par 3^200, mais pas par 3^{201}.

Exercice 9 Trouver tous les entiers tels que $m^3 = 4n + 2$.

Solution de l'exercice 9 La valuation 2-adique de m^3 est un multiple de 3, mais $4n + 2$ est pair sans être multiple de 4. Ainsi, sa valuation 2-adique vaut 1, qui n'est pas un multiple de 3 : il n'existe pas de telle solution.

Exercice 10 Que vaut $\nu_2(2^{100} + 2^{200})$?

Solution de l'exercice 10 On a $2^{100} + 2^{200} = 2^{100} \times (1 + 2^{100})$, et $1 + 2^100$ est impair, donc 2^{101} ne divise pas $2^{100} + 2^{200}$, mais 2^{100} le divise. Donc $\nu_2(2^{100} + 2^{200}) = 100$

Principe de descente infinie

Exercice 11 Montrer que $\sqrt{2}$ n'est pas rationnel en utilisant le principe de descente infinie.

Solution de l'exercice 11 On suppose par l'absurde que $\sqrt{2} = \frac{p_1}{q_1}$ avec $p_1, q_1 > 0$. Alors $2q_1^2 = p_1^2$, et donc p_1 est pair, et s'écrit $2 \times p_2 = p_1$, avec $p_1 > p_2 > 0$. Alors $q_1^2 = 2p_2^2$, donc q_1 est pair et de même il s'écrit $2 \times q_2 = p_2$. Alors $\sqrt{2} = \frac{p_2}{q_2}$. On construit ainsi de suite p_k, q_k tels que $\sqrt{2} = \frac{p_k}{q_k}$ et $0 < \cdots < p_3 < p_2 < p_1$. C'est impossible car cela donnerait une suite infinie strictement décroissante d'entiers positifs. On peut aussi faire une peuve sans passer par un raisonnement par l'absurde : si $\sqrt{2} = \frac{p_1}{q_1}$, alors $2q^2 = p^2$, mais la valuation 2-adique du membre de droite est paire, et celle du membre de gauche est impaire, c'est impossible

Exercice 12 Trouver toutes les solutions entières de l'équation :

$$x^2 + y^2 = 3(u^2 + v^2)$$

Solution de l'exercice 12 On montre d'abord un premier résultat : si 3 divise x^2+y^2 alors 3 divise x et 3 divise y. En effet, les carrés modulo 3 valent toujours 0 ou 1. Ainsi la somme de deux carrés vaut zéro modulo 3 si et seulement si les deux carrés sont congrus à zéro modulo 3, d'où le résultat. Soient x, y, u, v des entiers non tous nuls. Alors 3 divise $x^2 + y^2$, donc x et y sont divisibles par 3 par le résultat précédant. Mais alors $3(u^2 + v^2)$ est divisible par 3^2, donc u et v sont divisibles par 3 (par le résultat précédant).

Ainsi x, y, u, v sont divisibles par 3, et $x' = \frac{x}{3}, y' = \frac{y}{3}, u' = \frac{u}{3}, v' = \frac{v}{3}$ satisfont la même équation. Ainsi ces quatre entiers sont divisibles par trois par le même raisonnement, et ainsi de suite. Ainsi x, y, u, v peuvent être divisés par 3^n pour tout entier n, donc ils sont tous nuls.

La seule solution est alors $(0, 0, 0, 0)$.

Exercice 13 Montrer que tout rationnel $\frac{a}{b}$ inférieur ou égal à 1 peut s'écrire sous la forme $\frac{1}{n_1} \cdots + \frac{1}{n_k}$ pour certains entiers k et $n_1, \cdots, n_k$.

Solution de l'exercice 13 On va utiliser l'algorithme suivant : considérons le plus petit entier n tel que $\frac{a}{b} > \frac{1}{n}$. Il satisfait alors, $an > b$, et $an - b < n$. Alors on écrit $\frac{a}{b} = \frac{1}{n} + \frac{b-an}{bn}$. On recommence avec la fraction, $\frac{b-an}{bn}$. Au bout d'un moment la fraction obtenue est nulle, car la suite des numérateurs est strictement décroissante. Alors on obtient une écriture de $\frac{a}{b}$ de la forme désirée (les entiers n_i sont bien distincts, car le reste $\frac{b-an}{bn}$ est inférieur à $\frac{1}{n}$ puisque $a < b$).

5 jeudi 25 matin : Vincent Jugé

Principe des tiroirs

Exercice 1 Paris compte deux millions d'habitants. Un être humain a, au plus, 600 000 cheveux sur la tête. Au vu de ces seules informations, combien peut-on trouver de parisiens qui ont exactement le même nombre de cheveux sur la tête ?

Exercice 2 On a jeté de la peinture noire sur le sol blanc d'une pièce carrée de 2 mètres de côté, n'importe comment. Montrer qu'il existe deux points de la même couleur dont la distance est exactement d'un mètre.

Exercice 3 À l'occasion d'un stage Animath, qui regroupe au moins deux stagiaires, la relation « se connaître » est symétrique : si x connaît y, alors y connaît x. Montrer que, parmi les stagiaires, il en existe deux qui connaissent exactement le même nombre de stagiaires.

Principe de récurrence

Exercice 4 On se donne deux nombres r et a. On pose $s_0 = a$ puis, pour tout $n \geqslant 0$, on pose $s_{n+1} = s_n + r$. Proposer une formule simple pour s_n, puis montrer qu'elle convient.

Exercice 5 On pose $t_0 = 0$ puis, pour tout $n \geqslant 0$, on pose $t_{n+1} = t_n + n$. Les entiers t_n sont appelés « nombres triangulaires » : pourquoi ? Montrer que, pour tout $n \geqslant 0$, on a $t_n = n(n+1)/2$.

Exercice 6 On pose $u_1 = 1/2$ puis, pour tout $n \geqslant 2$, on pose

$$u_n = u_{n-1} + \frac{1}{n(n+1)}.$$

Proposer une formule simple pour u_n, puis montrer qu'elle convient.

Exercice 7 Montrer que, pour tout $n \geqslant 1$, on a l'inégalité

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} \leqslant 2 - \frac{1}{n}.$$

Exercice 8 Sur une île déserte vit, en l'an 0, un couple de lapereaux qui viennent de naître. Chaque année, chaque couple de lapins âgés d'au moins deux ans se reproduit et engendre un nouveau couple de lapins. Ainsi, il y a un couple en l'an 0 ; un couple en l'an 1 ; deux couples en l'an 2 (un couple de lapereaux, et notre premier couple né en l'an 0, qui s'est reproduit) ; trois couples en l'an 3, etc. On note F_n le nombre de couples de lapins vivant en l'an n (la suite $(F_n)_{n\geqslant 0}$ est connue sous le nom de « suite de Fibonacci »).

1. Donner une formule simple pour définir F_n par récurrence, à partir de F_{n-1} et F_{n-2}.
2. On se trouve face à un escalier à trois marches. On a des jambes assez grandes pour monter les marches par une ou par deux, mais pas par trois. Montrer qu'il existe F_n manières différentes de monter l'escalier.

Descente infinie

Exercice 9 Soit (x, y, z) trois entiers solutions de l'équation $x^3 + 2y^3 = 4z^3$. Montrer que x est pair, puis identifier toutes les solutions de cette équation.

Invariants

Exercice 10 Peut-on recouvrir un échiquier 9×9 avec des dominos 1×2 ?

Exercice 11 Une feuille de papier est déchirée en trois parties. Ensuite, l'une de ces parties est déchirée de nouveau en trois parties, et ainsi de suite. Peut-on obtenir, en fin de compte, un total de cent parties ?

Exercice 12 Est-il possible de répartir les entiers $1, 2, \ldots, 33$ en 11 groupes disjoints de trois éléments chacun, de sorte que, dans chaque groupe, l'un des éléments soit la somme des deux autres ?

Exercice 13 Sur une île déserte vivent 34 caméléons. Au départ, 7 sont jaunes, 10 sont rouges et 17 sont verts. Lorsque deux caméléons de couleurs différentes se rencontrent, ils prennent tous les deux la troisième couleur. Lorsque deux caméléons de la même couleur se rencontrent, il ne se passe rien. Au bout d'un an, il se trouve que tous les caméléons sur l'île sont devenus de la même couleur. Laquelle ?

Inclusion-exclusion

Exercice 14 Combien y a-t-il d'entiers à 4 chiffres ou moins et qui ne sont divisibles ni par 3, ni par 5, ni par 7 ?

6 jeudi 25 après-midi : Raphaël Ducatez

Pot pourri d'exercices, d'arithmétique et de stratégies de base, issu d'autres polycopiés de stages Olympiques. François Lo Jacomo a remplacé Raphaël Ducatez après le goûter pour un dernier exercice (comment retrouver l'année de naissance à partir des autres chiffres et de la clef de contrôle du numéro de sécurité sociale).

IV. Avancés

1 mardi 23 matin : Baptiste Serraille

Premier cours de géométrie. Voir d'autres polycopiés de stages olympiques.

2 mardi 23 après-midi : Cécile Gachet

Cours d'arithmétique et d'inégalités qui reprend des exercices publiés par ailleurs dans d'autres polycopiés d'Animath.

3 mercredi 24 matin : Baptiste Serraille

Deuxième cours de géométrie... Voir d'autres polycopiés de stages Olympiques...

4 mercredi 24 après-midi : Raphaël Ducatez

Exercices

Exercice 1 On souhaite ranger sur une étagère k livres de mathématiques (distincts), m livres de physique, et n de chimie. De combien de façons peut-on effectuer ce rangement :

1. si les livres doivent être groupés par matières ;
2. si seuls les livres de mathématiques doivent être groupés.

Exercice 2 Pour $n \in \mathbb{N}^*$, on note a_n le nombre de manières de recouvrir un rectangle de taille $2 \times n$ avec des pièces de taille 1×2. Trouver une relation de récurrence entre les a_n.

Exercice 3 On dispose d'un domino de largeur 1 et de longueur n. On note A_n le nombre de coloriages possibles de ce domino, c'est-à-dire le nombre de façons différentes de noicir ou non les cases. On note F_n le nombre de façons de colorier ce domino de telle sorte qu'il n'y ait jamais deux cases voisines noircies.

1. Calculer A_n.
2. Calculer F_1, F_2, F_3 et F_4.
3. Trouver une relation de récurrence entre les F_n.
4. Montrer que $\forall n \in \mathbb{N}^*,\ \forall p \in \mathbb{N}^*,\ F_{n+p+1} = F_n F_p + F_{n-1} F_{p-1}$.

Exercice 4 Soit n et k entiers tels que $1 \leqslant k \leqslant n$. Donner deux démonstrations de la formule suivante : $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \ldots + \binom{k}{k}$.

Exercice 5 Quel est le nombre de m-uplets $(x_1, x_2, \ldots, x_m) \in (\mathbb{N}^*)^m$ vérifiant $x_1 + \ldots + x_m = n$?

Exercice 6 Soit $n \in \mathbb{N}^*$. On se donne $2n$ points sur le bord d'un cercle. On note F_n le nombre de façons de relier ces points, deux à deux, à l'aide de n cordes qui ne se recoupent pas à l'intérieur du cercle. Trouver une relation de récurrence entre les F_n.

Exercice 7 Soit $n \geqslant 1$. Montrer que $\displaystyle\sum_{k=1}^{n} \binom{n}{k} k^2 = n(n+1)2^{n-2}$.

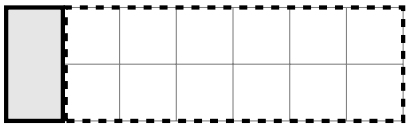
Exercice 8 Soit $n \in \mathbb{N}$. Montrer que $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

Solutions des exercices

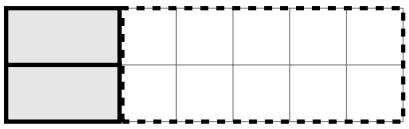
Solution de l'exercice 1

1. D'abord choisir l'ordre des matières (3! choix), puis pour chaque matière l'ordre des livres ($k!m!n!$ choix). Cela fait au total : $3!k!m!n!$ façons de ranger les livres.
2. On peut d'abord ne considérer que les livres de physique et de chimie. Ils sont au nombre de $n+m$. Il y a donc $(n+m)!$ façons de les ordonner. Il y a ensuite $(n+m+1)$ emplacements pour insérer le groupe des livres de mathématiques (tout à gauche, tout à droite, et entre deux livres consécutifs). Il faut enfin choisir un ordre pour les livres de mathématiques ($k!$ choix). Conclusion, il y a $(n+m+1)!k!$ façons de ranger les livres.

Solution de l'exercice 2 Posons $a_0 = 0$. On a clairement $a_1 = 1$. Pour $n \geqslant 2$, regardons ce qui peut se passer tout à gauche du rectangle. Soit on place une pièce verticale,



et il reste ensuite un rectangle de taille $2 \times (n-1)$ qui se recouvre de a_{n-1} façons différentes ; ou bien, on place deux pièces horizontales,



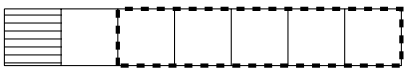
auquel cas il reste un rectangle de taille $2 \times (n-2)$ qui se recouvre de a_{n-2} manières différentes. Conclusion, on a la relation :

$$a_n = a_{n-1} + a_{n-2}.$$

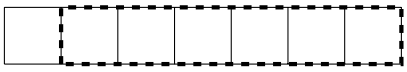
Solution de l'exercice 3

1. Pour chaque case, on peut choisir de la colorier ou non (2 choix). On a donc $A_n = 2^n$.

2. On trouve facilement $F_1 = 2$, $F_2 = 3$, $F_3 = 5$, $F_4 = 8$.
3. Prenons $n \geqslant 3$ et distinguons deux cas. Si la première case est noircie, la deuxième ne doit pas l'être.



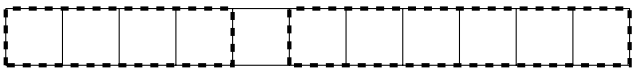
Il reste ensuite un domino de longueur $n-2$ qu'on peut colorier sans contrainte particulière (F_{n-2} choix). Si la première case n'est pas noircie, il n'y pas pas de contrainte sur la deuxième, et il reste donc un domino de longueur $n-1$ à colorier (F_{n-1} choix).



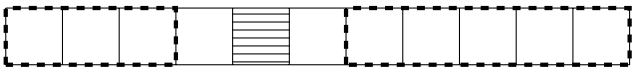
Conclusion, pour $n \geqslant 3$, on a la relation :

$$F_n = F_{n-1} + F_{n-2}.$$

4. Soient $n \geqslant 1$ et $p \geqslant 1$. On se donne un domino de longueur $n+p+1$ et on considère la $(n+1)$-ième case. Si on choisit de ne pas colorier celle-ci, il y a alors à gauche un domino de longueur n et à droite un domino de longueur p qu'on peut colorier sans contrainte particulière. Cela fait en tout F_nF_p choix.



Si on choisit de la colorier, ses voisines doivent rester blanches, et on a alors des dominos de longueur $n-1$ et $p-1$ à respectivement à gauche et à droite à colorier sans contrainte particulière. Cela fait $F_{n-1}F_{p-1}$ choix.



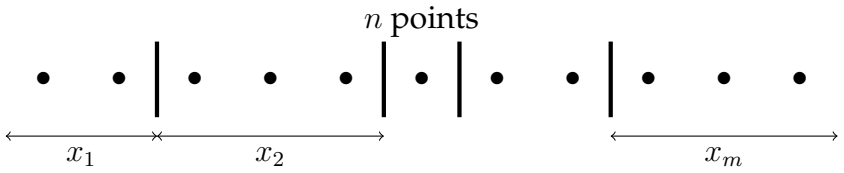
Conclusion, on a bien :

$$F_{n+p+1} = F_nF_p + F_{n-1}F_{p-1}.$$

Solution de l'exercice 4 Le premier terme compte le nombre de sous-ensembles de $\{1, \dots, n+1\}$ à $k+1$ éléments. Comptons ces derniers d'une autre façon, et les partionnant selon le plus petit élément qu'ils contiennent. Les sous-ensembles dont le plus petit élément est 1 et contenant $k+1$ éléments sont au nombre de $\binom{n}{k}$. En effet, se donner un tel sous-ensemble revient à choisir k éléments dans $\{2, \dots, n+1\}$ (le 1 étant déjà donné). De même, les sous-ensembles à $k+1$ éléments et donc le plus petit élément est 2 sont au nombre de $\binom{n-1}{k}$. Et ainsi de suite. Finalement, on obtient bien :

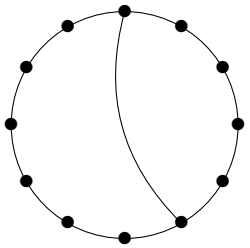
$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{k}{k}.$$

Solution de l'exercice 5 A chaque m-uplet $(x_1, \dots, x_m)$ d'entiers strictement positifs tels que $x_1 + \cdots + x_m = n$, on peut associer la représentation suivante.



Se donner un m-uplet qui convient revient à choisir les emplacements des $m-1$ séparations. Or il y a $n-1$ emplacements possibles. La réponse est donc $\binom{n-1}{m-1}$.

Solution de l'exercice 6 Choisissons un point arbitrairement, par exemple celui se trouve en haut du cercle. Et on partitionne les configurations selon le point auquel le premier est relié. La corde concernée sépare la configuration en deux.



Notons k la moitié du nombre de points se trouvant strictement à droite de cette corde. k varie donc de 0 à $n-1$. Les $2k$ points à droite de la corde peuvent être reliés de F_k façons et ceux à gauche de F_{n-k-1} façons. Conclusion, on a

$$F_n = \sum_{k=0}^{n-1} F_k F_{n-k-1}.$$

Solution de l'exercice 7 Dans la somme de gauche, chaque terme compte la façon de choisir une équipe de k personnes parmi n, puis de désigner un capitaine et un gardien (qui peuvent être la même personne). La somme compte donc toutes les façons de constituer de telles équipes de tailles allant de 1 à n. Procédons maintenant à un comptage différent. Distinguons deux cas. Si le capitaine et le gardien sont la même personne, on peut commencer par désigner celle-ci (n choix). On désigne ensuite le reste de l'équipe, autrement dit, on choisit un sous-ensemble des $n-1$ personnes restantes (2^{n-1} choix). Cela fait donc $n2^{n-1}$ choix. Si le capitaine et le gardien sont distincts, on peut commencer par choisir le capitaine (n choix), puis le gardien ($n-1$ choix), et enfin le reste de l'équipe (2^{n-2} choix) ; cela fait donc $n(n-1)2^{n-2}$ choix. Finalement, on a bien

$$n2^{n-1} + n(n-1)2^{n-2} = n(n+1)2^{n-2}.$$

Solution de l'exercice 8 Le terme de droite compte le nombre de façons de choisir n personnes parmi $2n$. Imaginons qu'il y a n hommes et n femmes. On peut alors compter le nombre de façon de choisir k hommes ($\binom{n}{k}$ choix) et $n-k$ femmes ($\binom{n}{n-k} = \binom{n}{k}$ choix), puis sommer sur toutes les possibilités de k, c'est-à-dire de 0 à n :

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

5 jeudi 25 matin : Louise Gassot

Exercice 1 Trouver les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que $f(2n) = 2f(n)$ et $f(2n+1) = 2f(n)+1$ pour tout $n \in \mathbb{N}$.

Exercice 2 (Équation de Cauchy) Trouver les fonctions $f : \mathbb{Q} \to \mathbb{R}$ telles que $f(x+y) = f(x)+f(y)$ pour tous $x, y \in \mathbb{Q}$.

Exercice 3 Trouver les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que $f(f(n)) = n+1$ pour tout $n \in \mathbb{N}$.

Exercice 4 (Bonus) Trouver les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que $f(f(n)) = n+2019$ pour tout $n \in \mathbb{N}$.

Exercice 5 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous $x, y \in \mathbb{R}$,

$$f(x)f(y) + f(x+y) = xy.$$

Exercice 6 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous $x, y \in \mathbb{R}$,

$$f(x - f(y)) = 1 - x - y.$$

Exercice 7 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous $x, y \in \mathbb{R}$,

$$f(x^{333} + y) = f(x^{2018} + 2y) + f(x^{42}).$$

Exercice 8 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous $x, y \in \mathbb{R}$,

$$(x-y)f(x+y) - (x+y)f(x-y) = 4xy(x^2 - y^2).$$

Solutions

Solution de l'exercice 1 Soit f une éventuelle solution du problème. D'après les relations données, on voit bien que si l'on connaît les premières valeurs de f, on va pouvoir en déduire toutes les valeurs de f de proche en proche.

On commence donc par choisir $n = 0$, et l'on obtient $f(0) = 2f(0)$ d'où $f(0) = 0$.
Pour $n = 1$, on a $f(1) = f(2+1) = 2f(0)+1 = 1$
Pour $n = 2$, on a $f(2) = f(2) = 2f(1) = 2$
Pour $n = 3$, on a $f(3) = f(2+1) = 2f(1)+1 = 3$...
Il semblerait que $f(n) = n$ pour tout n. C'est vrai pour $n = 0, 1, 2, 3$. Fixons un $n > 1$ et supposons que $f(k) = k$ pour tout $k \leq n$. On va prouver que $f(n+1) = n+1$.

— 1er cas : si $n+1$ est pair. Alors $n+1 = 2a$ pour un certain entier a tel que $0 \leq a \leq n$, et donc $f(a) = a$. Par suite, $f(n+1) = f(2a) = 2f(a) = 2a = n+1$.

— 2ème cas : si $n+1$ est impair. Alors, par construction, $f(n+1) = 2f(n/2)+1 = n+1$.

Donc dans tous les cas, $f(n+1) = n+1$. Finalement, de proche en proche, on a $f(n) = n$ pour tout n. Réciproquement, il est clair qu'une telle fonction est bien solution du problème, et il y a donc une seule solution qui est la fonction $n \mapsto n$.

Solution de l'exercice 2 Soit f une solution éventuelle du problème.

- Pour $x = y = 0$, il vient $f(0) = 2f(0)$, d'où $f(0) = 0$.
- En choisissant $y = -x$, on constate que, pour tout entier x, on a $f(x) + f(-x) = 0$, et donc que $f(-x) = -f(x)$. Cela assure qu'il suffit de déterminer f sur les entiers naturels pour connaître f sur $\mathbb{Z}$ tout entier.
- On ne voit pas de relation évidente pour déterminer $f(1)$, donc on pose $a = f(1)$.
- En choisissant $y = 1$, on constate que $f(x+1) = f(x) + f(1) = f(x) + a$, pour tout entier x. Il est alors assez facile d'en déduire que $f(2) = 2a$, $f(3) = 3a$, $f(4) = 4a$. De proche en proche, on en déduit que $f(n) = na$ pour tout entier naturel n, puis pour tout entier relatif n.
- Si q est un rationnel, on peut écrire $q = \frac{m}{n}$ où m, n sont des entiers tels que $n > 0$. Puisqu'on connaît bien f sur les entiers, l'idée est de s'y ramener et pour cela, on constate que pour $x = y$, on a $f(2x) = 2f(x)$ puis, pour $y = 2x$ que $f(3x) = 3f(x)$, et de proche en proche que, pour tout entier $k > 0$ et tout rationnel x, on a $f(kx) = kf(x)$. Par suite, on a $f(nq) = nf(q)$ et aussi $f(nq) = f(m) = ma$, donc $nf(q) = ma$, d'où $f(q) = \frac{m}{n}a = qa$.

Ainsi, il y a une infinité de solutions, qui sont les fonctions de la forme $f : q \mapsto aq$ où a est un réel fixé.

Solution de l'exercice 3 Soit f une éventuelle solution. En composant l'équation fonctionnelle par f, $f(f(f(n))) = f(n+1) = f(n) + 1$ pour tout n. Cela implique que $f(n) = n + f(0)$ pour tout n, mais alors $f(f(n)) = n + 2f(0)$ pour tout n. Or $f(0)$ étant entier, $2f(0)$ ne peut pas être égal à 1.

Solution de l'exercice 4 On considère $g : \mathbb{Z}_{2019} \to \mathbb{Z}_{2019}$ définie par

$$g(n) = f(n \text{ [mod 2019]}) \text{ [mod 2019]}.$$

On montre que cette fonction est bien définie. On a $f(k) + 2019 = f(f(f(k))) = f(k + 2019)$ donc si $x \equiv y$ [mod 2019], alors $f(x) \equiv f(y)$ [mod 2019] donc g est bien définie.

D'après l'égalité de l'énoncé, g est une involution, or $\mathbb{Z}_{2019}$ est de cardinal impair, donc g admet un point fixe $\overline{p} \in \mathbb{Z}_{2019}$, où p est un représentant de $\overline{p}$ dans $\mathbb{Z}$. Il existe alors un $k \in \mathbb{N}$ tel que $f(p) = p + 2019k$.

Or $f(f(p)) = p + 2019$ et $f(f(p)) = f(p + 2019k) = f(p) + 2019k$. D'autre part, en itérant l'égalité $f(x + 2019) = f(x) + 2019$, on obtient $f(f(p)) = p + 2 \times 2019k$, d'où $p + 2019 = p + 2 \times 2019k$ et $k = \frac{1}{2}$, absurde ! Ainsi cette équation n'a pas de solution.

Remarquons que le raisonnement tient toujours en remplaçant 2019 par n'importe quel nombre impair, mais l'équation fonctionnelle $f(f(x)) = x + 2n$ où n est un entier naturel fixé a toujours au moins une solution $f : k \mapsto k + n$.

Solution de l'exercice 5 En prenant $x = 0$, on a $(f(0) + 1)f(y) = 0$. Comme f ne peut pas être identiquement nulle (prendre $x = y = 1$ par exemple), on a $f(0) = -1$. En prenant $x = -y = 1$, on a $f(1)f(-1) = 0$.

Si $f(1) = 0$, en prenant $x = 1$, on a $f(y + 1) = y$, donc la seule fonction solution possible est $x \mapsto x - 1$. On vérifie qu'elle convient.

Sinon, $f(-1) = 0$, et en prenant $x = -1$, on trouve de même $x \mapsto -1 - x$ comme unique possibilité, et elle convient également.

Solution de l'exercice 6 Soit f une éventuelle solution.

En prenant $x = f(y)$ dans l'équation de départ, on obtient $f(y) = 1 - f(0) - y$. Ainsi, f est de la forme $x \mapsto c - x$ avec $c = 1 - f(0)$. En réinjectant dans l'équation initiale, on en déduit que pour tous réels x, y, $c - (x - (c - y)) = 1 - x - y$. Par conséquent, $c = \frac{1}{2}$, et l'on vérifie que $x \mapsto \frac{1}{2} - x$ est bien solution.

Solution de l'exercice 7 Parfois une simple substitution permet de tuer une équation fonctionnelle qui a l'air méchante... Soit f une solution éventuelle. On veut une substitution qui puisse tuer deux termes... testons la méthode la plus simple : $x^{333} + y = x^{2018} + 2y$ lorsque $y = x^{333} - x^{2018}$, pourquoi ne pas poser $y = x^{333} - x^{2018}$? On obtient directement $f(x^{42}) = 0$ pour tout réel x. Ainsi f est nulle sur les réels positifs.

En posant $y = 0$, on a $f(x^{333}) = f((-x)^{333})$ donc f est nulle sur $\mathbb{R}$ tout entier. La fonction nulle est donc l'unique solution. (La vérification est immédiate).

Solution de l'exercice 8 Pour clarifier un peu le problème, on pose $x + y = a$ et $x - y = b$. Ainsi $x^2 - y^2 = ab$, $2x = a + b$ et $2y = a - b$. On obtient pour tous réels a, b : $bf(a) - af(b) = ab(a^2 - b^2)$. En prenant $a = 0$, $bf(0) = 0$ pour tout b donc $f(0) = 0$.

Ensuite, pour $a, b \neq 0$, on divise par ab : $\frac{f(a)}{a} - \frac{f(b)}{b} = a^2 - b^2$, soit $\frac{f(a)}{a} - a^2 = \frac{f(b)}{b} - b^2$. La quantité $\frac{f(a)}{a} - a^2$ est indépendante du paramètre choisi ! On l'appelle $c = \frac{f(a)}{a} - a^2$ (valable pour tout a non nul). Ainsi pour tout $x \neq 0$, $f(x) = x^3 + cx$, mais cela reste valable pour $x = 0$ car $f(0) = 0$. Il ne reste plus qu'à vérifier que ces fonctions conviennent !

6 jeudi 25 après-midi : Thomas Budzinski

Ce cours de combinatoire reprend des exercices que vous trouverez par ailleurs dans d'autres polycopiés d'Animath.

V. Dernier jour : schibboleth de fin de stage

1 Énoncés

1 Débutants

Exercice 1 On définit les nombres u_n comme suit : $u_1 = 1$ et pour tout n, on a $u_{n+1} = u_n + 2n + 1$.

1. Calculer u_2, u_3 et u_4.
2. Conjecturer une formule et la montrer par récurrence.
3. Calculer u_{20}.

Exercice 2

1. Pour quelle valeurs de $n \in \mathbb{N}$, $6^{11} + 5n + 2$ est-il divisible par 7 ?
2. Quel est le reste de la division euclidienne de 39457^{27} par 11 ? par 9 ?

Exercice 3 Soit ABC un triangle, H son orthocentre, et M le milieu du segment $[BC]$. Appelons α la mesure de l'angle $\widehat{BAC}$.

1. Montrer que $\widehat{BHC} = 180 - \alpha$
2. Soit P le symétrique de H par rapport à (BC). Montrer que A, B, C et P sont cocycliques (pas nécessairement dans cet ordre !)
3. Soit Q le symétrique de H par rapport à M. Montrer que A, B, C et Q sont cocycliques (encore une fois, pas nécessairement dans cet ordre !)

On rappelle que faire une figure est indispensable.

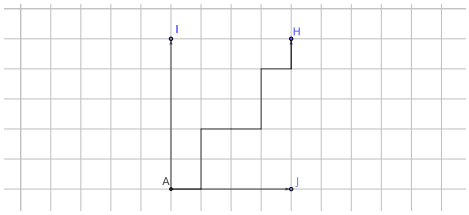
Exercice 4 Alice écrit au tableau 11 entiers deux à deux distincts, entre 1 et 20 inclus.

1. Existe-t-il forcément deux entiers écrits au tableau dont la différence est 10 ?
2. Existe-t-il forcément deux entiers écrits au tableau dont la différence est 9 ?

2 Avancés

Exercice 1 Une fourmi se trouve sur le point A (voir la figure ci-dessous) et souhaite aller jusqu'au point H. Elle se déplace sur une grille et à chaque minute, elle se déplace d'une case soit vers la droite soit vers le haut (et jamais à gauche ou en bas). Le point H se trouve n cases plus haut et k cases à droite par rapport à A. Autrement dit, dans le repère indiqué sur la

figure, on a $A = (0, 0)$ et $H = (k, n)$. Combien y a-t-il de chemins possibles pour la fourmi pour aller de A à H ?



Exercice 2 Le but de l'exercice est de trouver les fonctions $f : \mathbb{R}^* \to \mathbb{R}$ qui vérifient

$$f(x) + 3f(\frac{1}{x}) = x^2$$

pour tout $x \in \mathbb{R}^*$.

1. Montrer que $f\left(\frac{1}{x}\right) = \frac{1}{x^2} - 3f(x)$
2. Montrer alors que la seule fonction possible est $f(x) = -\frac{x^2}{8} + \frac{3}{8x^2}$

Exercice 3 Sur une table se trouvent 2018 jetons. Tour à tour, Alice et Bob doivent enlever un certain nombre de jetons. Plus précisément, à son tour, un joueur doit retirer au moins un jeton, et au maximum la moitié des jetons restants sur la table. Le joueur qui laisse un unique jeton sur la table perd la partie. C'est Alice qui commence. Déterminer lequel des deux joueurs possède une stratégie gagnante.

Exercice 4 Soit ABC un triangle, et P un point du segment $[BC]$ tel que les rayons des cercles inscrits aux triangles ABP et ACP soient égaux. Montrer que les rayons des cercles A-exinscrits dans les triangles ABP et ACP sont également les mêmes.

Remarque

Le cercle A-exinscrit dans le triangle ABP est le cercle tangent aux prolongements des côtés $[AP]$ et $[AB]$ au delà de B et P et aussi au côté $[BP]$. De même, le cercle A-exinscrit dans le triangle ACP est le cercle tangent aux prolongements des côtés $[AP]$ et $[AC]$ au delà de P et C, et aussi au côté $[CP]$.

VI. Conférences

1 Mardi soir : Codes secrets (Razvan Barbulescu)

L'humanité a utilisé différentes méthodes pour protéger ses communications. Si à la Préhistoire la multitude des langues permettait de garder le secret dans un groupe restreint, les méthodes modernes sont toutes basées sur les mathématiques.

Les Spartiates. En 404 av. J.-C. les Spartiates ont utilisé une méthode qui revient à écrire les lettres d'un texte à des intervalles réguliers, disons toutes les trois positions. Quand on arrive à la fin de la ligne on recommence pour remplir les espaces restés vides. La clé secrète est le nombre de cases à sauter, laissant très peu de possibilités à essayer.

César. Lors de ses campagnes, Jules César chiffrait les messages en décalant les lettres d'un nombre de positions. Par exemple si on choisit de décaler de 2, tous les A deviennent des C, tous les B des D etc. La sécurité est le nombre de décalages possibles : 25.

Substitution. On écrit les lettres de l'alphabet sur une ligne. Ensuite on choisit un ordre des lettres au hasard et on l'écrit sur la 2e ligne. Pour chiffrer un texte, tous les A sont remplacés par la lettre écrite en dessous de A et de même pour les autres lettres. Le nombre de possibilités à essayer est le nombre de façons de ranger 26 lettres, qui est $26! = 1 \cdot 2 \cdots 25 \cdot 26 \approx 4 \cdot 10^{26}$, ce qui prendrait 4300 ans à un million d'ordinateurs de fréquence 3 GHz. Mais Al-Kindi a écrit comment casser sans essayer toutes les possibilités : la lettre la plus fréquente dans le texte est le chiffré de la lettre la plus fréquente en français : "e" dont la fréquence est 15%.

Automatisation : Enigma. Pour contrecarrer la méthode d'Al-Kindi, il faut que le chiffré d'une lettre dépende de sa position dans le texte : on utilise un cahier avec une substitution par page, on chiffre la 1ère lettre à l'aide de la 1ère page, la 2e lettre à l'aide de la 2e page etc. Cela est très compliqué à réaliser et les cryptologues ont essayé des methodes qui miment cela, l'exemple le plus important étant Vigenère. Néanmoins, les seuls chiffres qui ont résisté à l'épreuve du temps sont ceux qui utilisent des machines (ou ordinateurs) réalisant des changements suffisamment compliqués pour ne pas être cassés, mais qui restent simple à utiliser. La machine Enigma, utilisée par les Allemands lors de la guerre, a été cassée par les Polonais puis, après modification, par les Anglais.

Masque jetable. Suite à cette longue liste de chiffres cassés, on peut se demander s'ils sont tous vulnerables. La réponse est non car on peut utiliser le masque jetable. Pour l'utiliser on

a besoin d'avoir échangé un texte suffisamment long, appelé masque. Pour chiffré on fait la somme entre le texte à chiffrer et le masque, lettre par lettre, en considérant A=1, B=2, etc. C'est le chiffre utilisé par certains espions, les messages chiffrés étant envoyés par la radio. Le téléphone rouge entre le président Américain et Russe chiffre ses message par le masque jetable.

Cryptographie asymétrique. Même le masque jetable a un inconvéniant : on doit échanger une information secrète avant de commencer à communiquer, ce qui n'est pas possible sur internet. La solution a été proposée par Diffie et Hellman en 1976 et récompensée par le prix Turing, véritable Nobel de l'informatique. Si Alice veut recevoir des messages, elle envoit un coffre avec un cadenas ouvert dont elle garde la clé. Tout le monde peut mettre des messages dans le coffre et le fermer, mais elle est seule à pouvoir l'ouvrir. Le cadenas et la clé sont réalisés par des calculs mathématiques. Les cartes bancaires et les communications https (http sécurisé) sur internet utilisent cette cryptographie.

Cryptologie moderne. Les chercheur.e.s développent des nouvelles méthodes pour chiffres de façon que le chiffré de la somme soit la somme des chiffrés. Cela permet de faire les calculs dans des centres de façon moins gourmande en énergie. Une autre possibilité est celle du vote par internet.

Les codes secrets ont parcouru un long chemin et la cryptologie ne fait que se diversifier et ouvrir des nouvelles possibilités.

2 Mercredi soir : Animath (Matthieu Lequesne)

Vous avez tous reçu, avec le livret d'accueil, un tract présentant les actions d'Animath et de l'IOI. Ce sont ces mêmes actions qui ont été présentées oralement par Matthieu Lequesne. Vous pouvez également consulter le site : `animath.fr`, ainsi que le site de la préparation olympique : `maths-olympiques.fr`.