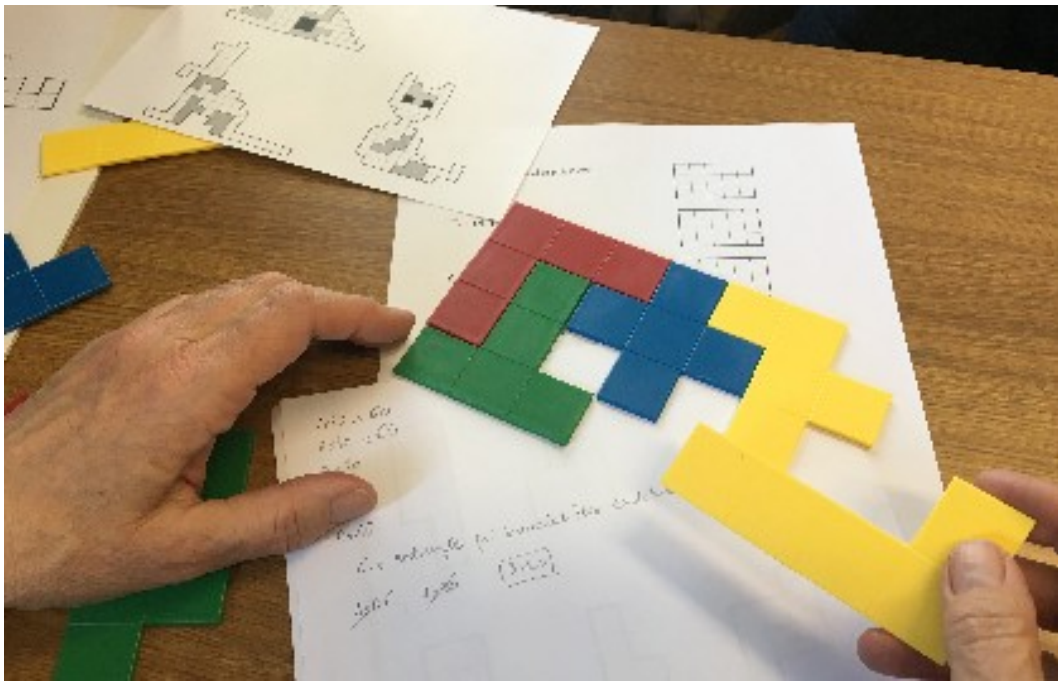
LE PETIT VERT

Bulletin de la Régionale Lorraine APMEP

N° 134	JUIN 2018



"Construire, manipuler, jouer et apprendre avec des polyminos" lors de notre JR.

N° ISSN : 0760-9825. Dépôt légal : juin 2018. Directeur de la publication : Gilles WAEHREN.
Pour les adhérents lorrains de l'APMEP, à jour de leur cotisation, l'abonnement au Petit Vert est gratuit. Il est proposé en version électronique (PDF). Cependant, (seulement si vous n'êtes plus en activité et si vous n'avez pas d'adresse électronique), vous pouvez demander une version papier expédiée par la poste (en format réduit et sans la couleur) ; pour cela, envoyez une demande à jacverdier@orange.fr. Les adhérents qui sont mutés dans une autre académie peuvent demander de continuer à recevoir le Petit Vert (version électronique PDF uniquement).

www.apmeplorraine.fr

SOMMAIRE

retour au sommaire

ÉDITORIAL

DANS MOINS DE QUATRE MOIS…

La réforme du lycée général est actée, mais nous ne voyons toujours pas de changement de programmes poindre à l'horizon. Peut-être ne porteront-ils que sur le format des cahiers des élèves : A4 ou européen. La question se pose alors de savoir si l'on peut envisager un changement aussi conséquent du lycée sans modification des contenus. Sur le papier, cela semble faisable. Mais, ce serait sans compter les mutations profondes qu'a impulsées la réforme du collège. Il serait temps de s'adapter à ce mouvement pour ne pas perpétuer les disparités entre élèves que la réforme du lycée veut diminuer.

L'évolution des notions a, en partie, été amorcée avec les quelques aménagements du programme de seconde, parmi lesquels, la partie « algorithmique » a connu des modifications dont nous n'avons pas encore pris toute la mesure. Nous ne pouvons cependant pas nous en tenir à la suppression de tel ou tel chapitre ou à l'apparition de tel ou tel autre. Nos élèves ont aussi besoin qu'on leur apprenne à gérer la masse d'informations directement accessibles sur Internet pour, par exemple choisir, selon leur goût, tel ou tel site de mathématiques. Nous ne pouvons pas ignorer cet immense réservoir documentaire : il serait bon d'enseigner des méthodes de recherche pertinentes et utiles. Nous nous efforçons tous les jours de faire le lien entre des notions, parfois éloignées en apparence, et ce travail demande un long temps d'apprentissage. L'École permet aussi de construire et d'exercer son sens critique, notamment par la confrontation de sources d'informations variées ; et les mathématiques nous apprennent notamment à nous méfier de ce que l'on croit avoir vu dans une figure, de ce que l'on pense avoir découvert dans un calcul. Nous devons continuer d'aider l'élève à apprendre par lui-même, lui donner les moyens de son autonomie. Autant de méthodes, qui paraissent parfois des vœux pieux dans les demandes des programmes et sur lesquelles il faut rester centré.

Pour les nouveaux contenus du programme de seconde, par exemple et parce qu'il faudrait qu'il soit mis en œuvre dans quatre mois, je suggère, puisque rien ne m'a encore été proposé, de supprimer les vecteurs (laissons-les aux premières 'scientifiques') et les fonctions du second degré. Cela devrait laisser du temps pour refaire de la géométrie (nostalgisme qui devrait ravir notre ministre) euclidienne et, surtout, dynamique. Cette partie des mathématiques permet de travailler les six compétences de façon active. Son intérêt technique a pu échapper à certains ; pourtant, je pense qu'on a voulu s'en débarrasser trop vite. N'est-il pas dommage de ne pas réinvestir ce que les collégiens ont vu sur les transformations, le théorème de Thalès et tous ceux qui lui sont liés ? Même après l'avoir enseignée plusieurs années, GeoGebra à l'appui, s'est-on vraiment lassé de la droite d'Euler (y compris avec les vecteurs) ? Les symétries de telle ou telle figure de l'espace ne sont-elles pas essentielles pour construire la vision d'une molécule ou pour réaliser une animation cinématographique assistée par ordinateur ? La géométrie nous sert souvent de support pour appréhender la notion de fonctions et, là encore, l'outil numérique apporte une plus-value dans la compréhension des phénomènes. Enfin, et la rubrique « sophismes » du Petit Vert ne manque jamais de le rappeler, la géométrie permet, comme évoqué ci-avant, de nous méfier des apparences trompeuses.

Vous aussi, devant l'absence de nouvelle proposition de programme, laissez libre cours à votre imagination pour construire une nouvelle progression qui donne du sens à notre enseignement !

president@apmeplorraine.fr

retour au sommaire

C'ÉTAIT IL Y A 25 ANS DANS LE PETIT VERT N°34 DE JUIN 1993

À propos des nouveaux programmes de lycée

Le nouveau ministre a tout chamboulé... A l'heure où nous mettons sous presse, nous ignorons tout des programmes qui seront mis en place à la rentrée prochaine. Tous ceux qui se sont investis, à l'A.P.M.E.P. comme ailleurs, dans les divers groupes de travail et de concertation voient leurs efforts anéantis ... et ne sont pas près de se remettre au travail.

A la Régionale Lorraine, nous avions obtenu de Monsieur le Recteur l'organisation de Journées académiques d'information sur les nouveaux programmes, et beaucoup de nos membres s'étaient donnés à fond pour les préparer. Hélas, nous avons dû tout annuler en dernière minute. Voici d'ailleurs la lettre écrite par Michèle FABREGAS[1] qui a été expédiée à tous les chefs d'établissement :
« Les contenus des programmes de mathématiques initialement prévus pour la rentrée 93 étant caducs, suite aux dernières décisions du Ministre de l'Éducation Nationale, l'équipe de formateurs reporte la formation à la rentrée prochaine. Les nouvelles dates, ainsi que les modalités d'inscription, seront communiquées ultérieurement. »

Extaits de l'éditorial du Petit Vert n°34

Il y a environ deux ans, j'ai eu l'occasion, avec quelques collègues de la Régionale, de rencontrer Monsieur l'Inspecteur Général OVAERT, qui nous a alors relaté l'anecdote suivante :

Le Ministre de l'Éducation Nationale venait de décider que les flux d'élèves entrant en classe de seconde des lycées devaient augmenter de 10 % par an pendant les quatre années suivantes, et demandait aux responsables de la Direction de la Prospective de lui calculer l'augmentation résultante de la population des lycées au bout de ces quatre années.

Réponses : 40 %, bien sûr (et point besoin d'une calculatrice) ... - Non, 46,41 %, Monsieur le Ministre (ceux-ci venaient de se souvenir qu'il fallait calculer $1{,}10^4$!!!).
Ces éminents personnages placés à la tête des rouages de l'État étaient tous des énarques (ce n'est pas moi qui l'affirme, c'est M. OVAERT), et je serais prêt à parier, quant à moi, qu'ils ont tous fait une terminale C...

Pour faire un petit peu de calcul, observons le lycée FICTIF, où il y a 100 élèves en seconde, autant en première et en terminale, et où personne ne redouble. Voici quelles y seraient les conséquences de la décision ministérielle :

	An. référence	An. + 1	An. + 2	An. + 3	An. + 4
Seconde	100	110	121	133	146
Première	100	100	110	121	133
Terminale	100	100	100	110	121
Total	300	310	331	364	400

L'augmentation n'y aura été que de 33 % (environ)... et non pas 40 %, bien sûr !

[1] Alors présidente de la régionale Lorraine.

retour au sommaire

VIE DE LA RÉGIONALE

LES MEMBRES DU COMITÉ POUR 2018/2019

Jean-Michel **BERTOLASO**, L.P. du Bâtiment, Montigny, J.Michel.Bertolaso@ac-nancy-metz.fr
Geneviève **BOUVART**, retraitée, gbouvart@wanadoo.fr
Ghislaine **BURKI**, en disponibilité, tresorier@apmeplorraine.fr
Sébastien **DANIEL**, collège Louis Armand, Petite-Rosselle, sebastien.daniel@rtvc.fr
Fathi **DRISSI**, collège Louis Armand, Moulin-lès-Metz, fathi.drissi@free.fr
François **DROUIN**, retraité, francois.drouin2@wanadoo.fr
Rachel **FRANÇOIS**, école primaire de Moyen, Rachel.Francois2@ac-nancy-metz.fr
Christelle **KUNC**, lycée Stanislas, Villers-lès-Nancy, christelle.kunc@wanadoo.fr
Michel **LEFORT**, collège Hauts-de-Blémont, Metz, michel.lefort@laposte.net
Laurent **MARX**, collège Les Gaudinettes, Marange-Silvange, laurent.marx@ac-nancy-metz.fr
Anas **MTALAA**, collège-lycée N-D.de la Providence, Thionville, anas.mtalaa@gmail.com
Pierre-Alain **MULLER**, lycée Nominé, Sarreguemines, pierre-alain.muller@wanadoo.fr
Walter **NURDIN**, ÉSPÉ de Lorraine, site Nancy, walter.nurdin@univ-lorraine.fr
Valérie **PALLEZ**, lycée Stanislas, Villers-lès-Nancy, valerie.pallez@ac-nancy-metz.fr
Aude **PICAUT**, lycée Mangin, Sarrebourg, aude.picaut@gmail.com
Michel **RUIBA**, retraité, michel.ruiba@ecopains.net
André **STEF**, F.S.T. et I.R.E.M., Univ. Lorraine, Vandœuvre, Andre.Stef@univ-lorraine.fr
Daniel **VAGOST**, retraité, daniel.vagost@gmail.com
Jacques **VERDIER**, retraité, jacverdier@orange.fr
Gilles **WAEHREN**, lycée Charles Mangin, Sarrebourg, president@apmeplorraine.fr
Stéphanie **WAEHREN**, collège Pierre Messmer, Sarrebourg, stephanie.waehren@wanadoo.fr

Les responsabilités dans la Régionale

Président d'honneur	Jacques VERDIER
Président	Gilles WAEHREN
Vice-président	Michel RUIBA
Trésorière	Ghislaine BURKI
Trésorier adjoint	Daniel VAGOST
Secrétaire	Geneviève BOUVART
Secrétaire adjoint	Sébastien DANIEL
Directeur de la publication « Le Petit Vert »	Gilles WAEHREN
Responsable commission Premier degré	Rachel FRANÇOIS
Responsable commission Collèges	Sébastien DANIEL
Responsable commission Lycées	Gilles WAEHREN
Responsable commission Lycées professionnels	Jean-Michel BERTOLASO
Responsable commission Enseignement supérieur	André STEF
Responsable commission Formation des maitres	Walter NURDIN
Responsable groupes "Jeux" et "Maths & Arts"	François DROUIN
Responsable rallye	Pierre-Alain MULLER
Responsable site internet.	Fathi DRISSI
Responsable comité de rédaction du Petit Vert	Jacques VERDIER
Responsable rubrique « problèmes »	Philippe FÉVOTTE
Chargé de mission brochures	Walter NURDIN

Chargés de mission Exposition itinérante : Andre.Stef@univ-lorraine.fr (54), joelle.agamis@free.fr (55), michel.ruiba@ecopains.net (57), baliviera.marie-jose@orange.fr (88) et pierre-alain.muller@wanadoo.fr (langues étrangères)

Vérificateurs des comptes : Marie-Claire KONTZLER et Christophe PRÉVOT

Le bilan d'activités et le bilan financier de l'année 2017 ont été envoyés par courriel à tous les adhérents à jour de leur cotisation. Ils ont été soumis au vote lors de l'Assemblée Générale du 21 mars 2018, et adoptés à l'unanimité. Ces bilans seront mis en ligne dès que le site sera opérationnel.

retour au sommaire

COMPTE RENDU DE LA JOURNÉE RÉGIONALE 2018

Cette journée s'est déroulée le 21 mars dernier, le matin à la Faculté des sciences, l'après-midi au lycée Callot. Un peu de statistiques : 198 inscrits, 168 présents. Parmi les présents, 84 adhérents. Pour 47 des présents, c'était leur première participation à cette journée.
73 participants ont pris le repas de midi au lycée Callot.

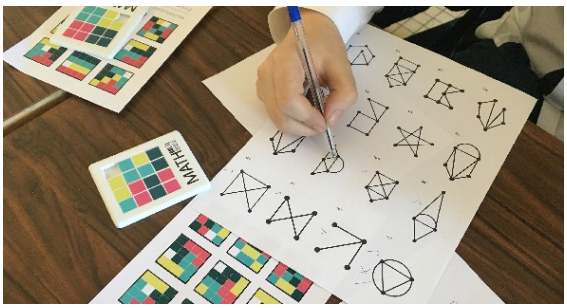
La conférence

Le repas au lycée Callot

La conférence inaugurale a été donnée par Frédéric Métin et Patrick Guyot, de l'université de Dijon, sur le thème « Didier Henrion, compilateur de récréations mathématiques des années 1620 ».
18 ateliers ont été proposés :

- Construire, manipuler, jouer et apprendre avec les pentaminos (26 participants)
- Calcul en ligne (9 participants)
- Je cherche, tu cherches, nous cherchons... ensemble (14 participants)
- Les Q.C.M. Interactifs (12 participants)
- Les mesures médiévales et la corde à 7 nœuds (10 participants)
- Infomagie : comment présenter les concepts informatiques (20 participants)
- Conserver un secret ? Grâce à la théorie des nombres (26 participants)
- Diagnostic instantané à l'époque 4.0 (14 participants)
- Aborder Python par l'aspect graphique et le travail sur l'image (11 participants)
- Entrée dans les problèmes par l'image (19 participants)
- Jouons les maths avec "Jeux école 3" (19 participants)
- Socrative, outil de questionnaire pour tablettes et smartphones (18 participants)
- Évaluation par compétences (12 participants)
- Souris, puisque c'est un graphe ! (21 participants)
- Algorithmique débranchée... le baseball multicolore revisité (11 participants)
- Lancer un club de maths au collège ou au lycée (11 participants)
- Scratch pour tous (7 participants)
- Python 3.4x avec Edupython (10 participants)

L'atelier « Ardoises Plickers »



L'atelier graphes

Trois de nos commissions régionales (Premier degré et collège, Lycée, Formation des maîtres et enseignement supérieur) se sont réunies ce jour. Vous trouverez leur comptes rendus ci-après. La journée s'est terminée par la réunion du Comité de notre régionale.

Rendez-vous à la Journée de 2019 (probablement le 20 mars).

La journée se déroulera entièrement au lycée Stanislas de Villers-lès-Nancy.

retour au sommaire

COMPTE RENDU DE LA COMMISSION RÉGIONALE ÉCOLE-COLLÈGE

(Journée régionale de l'APMEP du mercredi 21 mars 2018)

Lors de cette commission nous avons proposé une réflexion autour de plusieurs points d'actualités :

- le ressenti sur le terrain par rapport à la réforme au collège
- l'adaptation des programmes de 2nde
- un groupe de travail de Lorraine école-collège
- l'adaptation des programmes de 2nde / algorithmique
- la liaison école-collège en mathématiques

Concernant la poursuite de la mise en place de la réforme du collège on remarque une grande disparité sur l'utilisation de la marge horaire en mathématiques. On déplore que souvent cette répartition ne se fait pas du tout avec des objectifs pédagogiques mais uniquement avec soucis de donner des heures aux matières déficitaires.
On soulève une baisse régulière des horaires de mathématiques et demande est faite de plus d'heures de mathématiques pour nos élèves. Cette demande fait partie des revendications de l'APMEP (voir la plaquette Visages).

Plusieurs collègues nous font également part à nouveau de leurs inquiétudes concernant le matériel informatique. Souvent peu performant ou très limité, il ne permet pas un travail satisfaisant avec nos élèves sur les points du programme afférent. D'autres inquiétudes également à propos de la pertinence de l'usage des tablettes, souvent pointées comme matériel d'avenir par les collectivités territoriales.
Ces demandes avaient été remontées et figurent également dans les revendications de l'APMEP au niveau national.

Plusieurs collègues nous ont interrogé sur nos expositions « Jeux mathématiques » qui peuvent être réservées et utilisées avec nos élèves.
Les tarifs sont variables suivant les expositions, il suffit de nous contacter pour plus d'informations.
Il est également possible selon les disponibilités de vous accompagner dans la mise en place des ateliers avec vos élèves.
Une demande de création d'une liste des jeux de l'exposition itinérante a été faite et sera étudiée lors d'un prochain comité.

Nous avons rappelé la publication d'une adaptation des programmes de seconde suite aux nouveaux programmes des cycles de l'école et du collège, vous trouverez ces textes à l'adresse suivante : http://www.education.gouv.fr/pid285/bulletin_officiel.html?cid_bo=115984

Enfin nous avons rappelé qu'au niveau national une commission école-collège se réunit régulièrement pour réfléchir à l'enseignement des mathématiques dans les cycles 1 à 4 et produire des ressources à destination de nos collègues.
Il a été demandé si tous les adhérents peuvent y participer et la réponse est oui.
Nous proposons également aux collègues intéressés d'organiser une commission école-collège au niveau lorrain, en dehors de la journée régionale, qui pourrait faire part de nos revendications au niveau régional ou réfléchir à des productions pour les collègues. Le mode de fonctionnement est à inventer, toutes les idées seront accueillies avec enthousiasme.

Si vous souhaitez y participer n'hésitez pas à nous contacter : sebastien.daniel@rtvc.fr

retour au sommaire

COMPTE RENDU DE LA COMMISSION LYCÉE

(Journée régionale de l'APMEP du mercredi 21 mars 2018)

Une cinquantaine de personnes étaient présentes.
Gilles Waehren a rappelé des positions principales du comité national de l'APMEP sur la réforme du lycée (délai trop court ; pistes intéressantes sur la modularité avec des heures pour l'orientation mais avec un horaire réduit pour les disciplines et la difficulté pour un élève de seconde de se projeter trois années plus tard) et le communiqué du 19 mars.
Les changements pour l'année scolaire à venir en classe de seconde ont été précisés : 1,5 h hebdomadaire consacré à l'orientation ; Accompagnement Personnalisé essentiellement consacré à la maitrise de la langue et de l'oral. L'Accompagnement Personnalisé ciblé davantage pour les mathématiques semble disparaitre.
De nombreuses questions, inquiétudes et remarques ont été ensuite exprimées :

- **Sur la place des mathématiques au lycée**

Qui va faire encore des maths au lycée à partir de 2019 ? Les mathématiques ne sont pas dans le tronc commun.
Les mathématiques ne sont-elles qu'un outil pour le lycée ?
Y aura-t-il un nouveau programme de mathématiques ? Une différenciation dans les programmes ? Quel sera le contenu des humanités scientifiques et numériques ?

- **Sur la place de l'élève dans cette réforme**

Est-ce que tous les élèves ont besoin d'un enseignement de mathématiques ? Si oui, lequel ?
On peut ne pas faire de mathématiques avec des majeures physique-SVT. Cela peut-il donner un apprentissage scientifique efficace ?
Les lycéens ne peuvent pas vraiment mesurer les conséquences de leurs choix – voir le rapport Villani sur le niveau faible en mathématiques des professeurs des écoles. A contrario, dans notre enseignement, les choix sont souvent faits par défaut. Le côté positif de la réforme est de choisir réellement ses disciplines.

- **Sur l'organisation générale du lycée**

Si une discipline n'est pas choisie en première est-ce possible de la reprendre en terminale ?
Quelle est la place de la filière technologique dans cette réforme ?
Quelles sont les demandes du supérieur ?
Les couplages de matières ne sont pas tous possibles. Les choix vont être fonction des établissements. A Fameck, la cheffe d'établissement souhaite mettre en place tous les couplages en montrant l'importance des mathématiques.
Y aura-t-il des groupes ? Des dédoublements ?

- **Sur le rôle de l'enseignant**

Pouvons-nous êtres de bon conseil pour l'élève dans le choix de ses enseignements ?
Qui enseigne en informatique et sciences du numérique ?
y a–t-il suffisamment d'enseignants formés ?

retour au sommaire

LE RALLYE RÉGIONAL 2018

Participation au Rallye : 190 classes (en baisse depuis trois ans … il faudra réfléchir à la cause).

Année 2018	Collèges		Lycées		Total	
	Établissements	Classes	Établissements	Classes	Établissements	Classes
M. et Moselle	7	16	4	22	11	38
Meuse	4	12	2	4	6	16
Moselle	17	42	14	55	31	97
Vosges	8	26	2	13	10	39
Total	36	96	22	94	58	190

Les classes lauréates

Collèges

1er prix : classe de 3ème E, collège Nelson Mandela, VERNY (57)

2ème prix ex æquo : classe de 3ème A, collège Jules Ferry, BRIEY (54)

2ème prix ex æquo : classe de 3ème 1, collège Fleurot d'Hérival, LE VAL D'AJOL (88)

Lycées

1er prix : classe de 2ème 4, Lycée Louis Vincent, METZ (57)

2ème prix : classe de 2ème 7, Lycée Charlemagne, THIONVILLE (57)

3ème prix : classe de 2ème 4, Lycée Fabert, METZ (57)

Nos félicitations à tous les participants !

Les sujets de 2018 sont ici :
http://apmeplorraine.fr/doc/Rallye_Mathématique_de_Lorraine_2018.pdf
Les solutions sont là :
http://apmeplorraine.fr/doc/Rallye_solutions_2018.pdf

Dans le prochain Petit Vert, vous trouverez quelques commentaires concernant certains des exercices proposés.

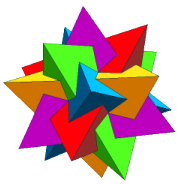
Nous rappelons les objectifs de ce rallye

Permettre à tous les élèves d'une classe de participer à une activité mathématique ;

Motiver les élèves par des jeux et des énigmes à résoudre ;

Favoriser la communication et la coopération au sein de la classe ;

Faire participer le plus d'élèves possible et aider ainsi à la liaison collège-lycée.



retour au sommaire

SÉMINAIRE DE RENTRÉE DE LA RÉGIONALE

Comme tous les deux ans, la Régionale de Lorraine organise un séminaire. Il aura lieu, cette année, le week-end du 25-26 août 2017 à Ramonchamp, dans le département des Vosges.
Le thème retenu cette année sera : "Un site pour la Régionale de Lorraine."

Le programme sera le suivant :
- samedi 14 h : Présentation de la structure du site et des manipulations techniques.
- samedi 16 h : Création des pôles de rédaction des différentes rubriques
- dimanche 9 h : Prise en main et publication des premiers contenus

Les fournitures de draps et les repas du samedi soir et dimanche midi sont assurés par le village vacances des 4 vents (http://www.vosges4vents.com/).
Les tarifs seront de 60 € par adulte, 30 € par enfant à régler lors du séjour. Si vous ne souhaitez pas être hébergé, vous pouvez tout de même vous inscrire et payer les repas (15 €).

Pour vous inscrire, vous devez impérativement remplir le formulaire à l'adresse : https://drive.google.com/open?id=1Ri2TeIi5C7-hwnC3VlV7NCHgobivfgzAiq9RNALv8hM

… AVANT LE 30 JUILLET 2018

Notre revue numérique nationale est opérationnelle depuis le 1er juin sur le site de l'APMEP.
Pour s'y rendre, allez sur le site de l'APMEP (page d'accueil) et cliquez sur l'onglet "Au fil des maths" ou https://afdm.apmep.fr/.

" LE PETIT VERT " est le bulletin de la régionale APMEP Lorraine.
Né en 1985, il complète les publications nationales que sont le bulletin « Au fil des maths » et le BGV. Il parait quatre fois dans l'année (mars, juin, septembre et décembre). Son but est d'une part d'informer les adhérents lorrains sur les activités de la Régionale et sur la "vie mathématique" locale, et d'autre part de permettre les échanges "mathématiques" entre les adhérents.
Il est alimenté par les contributions des uns et des autres ; chacun d'entre vous est vivement sollicité pour y écrire un article et cet article sera le bienvenu : les propositions sont à envoyer à jacverdier@orange.fr.

Le Comité de rédaction est composé de Geneviève Bouvart, François Drouin, Rachel François, Françoise Jean, Walter Nurdin, Michel Ruiba, Jacques Verdier et Gilles Waehren.
La maquette et la mise en page sont réalisées par Geneviève Bouvart et Michel Ruiba.

retour au sommaire

CHEZ NOS VOISINS ALSACIENS

Depuis quelques années, la régionale APMEP alsacienne tournait au ralenti, sans activités, avec une présidente démissionnaire depuis plusieurs mois. Les lorrains ont été invités le 9 avril dernier à participer à une journée (inscrite au PAF de l'académie de Strasbourg par l'IPR Michel Barthel, bien connu de nos adhérents lorrains) qui devait aider cette régionale à se « redynamiser » : nous étions venus avec quelques idées, les stands de notre exposition « Objets mathématiques » et les brochures éditées par notre régionale.

Les jeux tirés de nos valises lorraines « Objets mathématiques » ont eu un grand succès...

À l'issue de cette journée, un nouveau comité « provisoire » de 9 membres (dont cinq « nouveaux ») a été mis en place.

Le 25 mai, un nouveau comité a été constitué : présidente, Anne-France Acciari (professeure en collège) ; vice-président, Gilles Bergerat (professeur en collège) ; trésorier, Richard Cabassut (ÉSPÉ de Strasbourg) ; secrétaire, Serge Petit (retraité).

Les alsaciens prévoient déjà de proposer une journée régionale (inscrite au PAF) pour le printemps prochain. Peut-être quelques lorrains pourront-ils y animer un atelier (voire même plusieurs)...

Longue vie à cette régionale amie ...

retour au sommaire

ANIMATION : DES JEUX MATHÉMATIQUES À LA MATERNELLE

Le mercredi 21 février, notre régionale - représentée par trois adhérents grands joueurs - a participé à une animation pédagogique avec Canopé (site de Montigny-lès-Metz) et les CPC des circonscriptions de Metz-Est et Metz-Nord, à destination de tous les collègues PE en cycle 1 (PS, MS et GS de maternelle) des deux circonscriptions, au collège Jules Lagneau à Metz.

Cet après-midi ludique a été très apprécié par toutes et tous et a donné lieu à des échanges déjà fructueux.

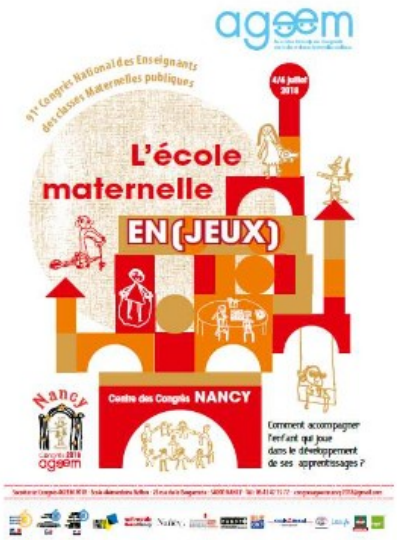
Les documents proposés lors de cette animation pédagogique :
https://www4.ac-nancy-metz.fr/ien57metzest/spip.php?article450&lang=fr

Vous pourrez retrouver ces jeux et d'autres ressources sur le site de l'**APMEP**, L'association des professeurs de mathématiques de l'enseignement public y propose de nombreuses ressources.

Les articles du Petit Vert (en particulier dans la rubrique Maths et Jeux), sont également une source d'activités sur le thème des jeux.

(...) pas de panique, monsieur l'inspecteur, il faut savoir jouer avec le savoir. Le jeu est la respiration de l'effort, l'autre battement du cœur, il ne nuit pas au sérieux de l'apprentissage, il en est le contrepoint. Et puis jouer avec la matière c'est encore nous entraîner à la maîtriser.

Chagrin d'école, Daniel Pennac



Notre régionale sera présente au congrès de l'AGEEM à Nancy, du 4 au 6 juillet.

Le thème des journées est le jeu en maternelle, occasion pour nous de présenter des ressources APMEP et de les mettre à disposition des professeurs des écoles.

retour au sommaire

LIEU INSOLITE POUR JEUX MATHÉMATIQUES

En accueillant vingt adultes venus des villages de la vallée et même un retraité de Nompatelize, Pierre Sarrazin, le commerçant, et Marie-Jo Baliviera, la prof de maths retraitée, étaient fiers d'avoir atteint leur objectif !
Il fallut disposer les tables devant le comptoir et les rayonnages. Le moindre recoin était occupé (...).
Pas de jeux de cartes. Des jeux artisanaux conçus et réalisés par l'Association lorraine des professeurs de mathématiques qu'on ne trouve pas dans le commerce.
Marie-Jo rentrait tout juste d'une journée passée à Metz dans le cadre de cette semaine nationale. Les adultes de la vallée ont ressenti les mêmes impressions que les lycéens. Un remue-méninges dans l'épicerie, mais ludique.
Avec une grosse dose d'observations, de raisonnements, de tâtonnements… et l'aide bienveillante de Marie-Jo, présente pour encourager, remettre sur les rails, rendre actif tout ce monde qui, avec des yeux d'enfants, découvrait les jeux en bois, en carton, en métal, aux formes géométriques et aux couleurs diverses, à emboiter, déplacer, juxtaposer...

Selon Marie-Jo, l'objectif est atteint : « *Je voulais prouver que les mathématiques ne sont pas ingrates, qu'elles ne doivent pas faire peur. Le côté ludique plait beaucoup. Personne ne se lasse, prenant la décision de repartir à zéro en cas d'échec. Ils ont apprécié l'animation. Les liens se tissent, faisant fi des conditions sociales et autres, devant un café, un thé, des gâteaux maison* ».
« *Je n'avais jamais fait ça, c'était très bien !* », conclut Fabien, face à la prof toute émue. « *C'est promis, on recommencera sur la terrasse, avec des nouveautés !* ».

Extraits de Vosges Matin du 21 Mars 2018

À l'épicerie de Pierre, on a participé en nombre à la Semaine nationale des mathématiques, y compris Marcelle Valentin, l'aînée de Bionville.

Photo Vosges Matin

retour au sommaire

LE PLAISIR DES JEUX MATHÉMATIQUES EN MATERNELLE

L'enthousiasme de Marie-José Baliviera pour donner du plaisir a gagné la classe de maternelle de Noémie Salzber, directrice. Et l'amour des mathématiques ne s'est pas démenti. En effet, dès que les jeux artisanaux ont été déposés sur les tables, et quelques uns seulement parmi les 57 disponibles, ce fut une grande joie chez les écoliers. Il leur fallait manipuler, emboiter, superposer, juxtaposer toutes sortes de figures géométriques colorées, réalisées le plus souvent en bois.

Un réel succès. « *Des jeux construits par des professeurs, car on n'en trouve pas dans le commerce* ». Petit clin d'œil de Marie-Jo à ses collègues de l'association des maths, implantée à Paris, disposant d'antennes dans les académies. « *S'il existe une maison des maths à Lyon, il n'en est rien ici !* », commente l'intervenante bénévole, venue d'Allarmont. Aimant les contacts humains, elle répond aux demandes des enseignants du primaire et des collèges. Comme le fait Odile, une collègue et amie, plutôt en Moselle.

À la maternelle, Camille et Jules reçoivent les conseils avisés de Marie-Jo dont les jeux mathématiques sont un régal pour les bambins.

L'atelier « jeux mathématiques » remporte un tel succès que chacun en oublie le temps de la récréation. C'est une manière active de travailler autrement. Et souvent de façon autonome pour l'élève. Bien que ludique, la séance a suscité concentration, persévérance, raisonnement.

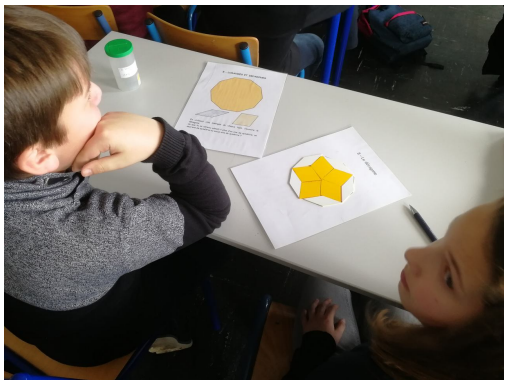
Un objectif atteint, selon les deux professeurs. « C'est positif, car l'enfant accepte de recommencer s'il ne réussit pas ! ».

Paru dans la Liberté de l'Est du 31 janvier.

* * * * * * * * *

SEMAINE DES MATHS À VAUCOULEURS

L'exemplaire meusien de l'exposition « Objets mathématiques » a été utilisé au collège "Les Cuvelles" par des élèves de CM2 et de 6ème le jeudi 15 mars et le lundi 19 mars 2018.

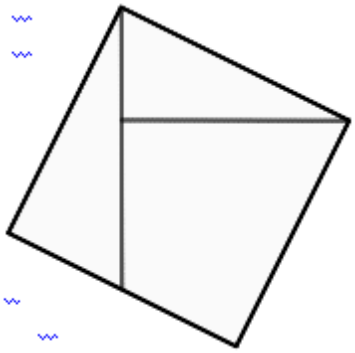


Le transfert s'est organisé du nord au sud du département.
Deux pièces endommagées ont été réparées : sa circulation peut continuer.

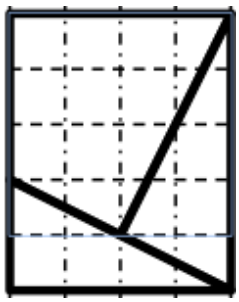
retour au sommaire

LE PUZZLE À TROIS PIÈCES EN CYCLE 1

Groupe Jeux et Maths - APMEP Lorraine

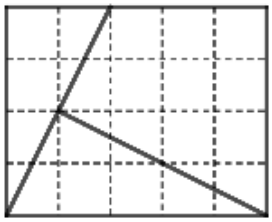
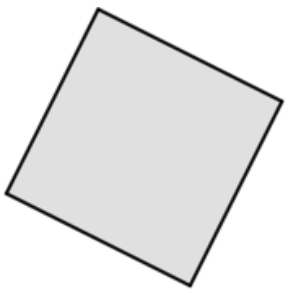
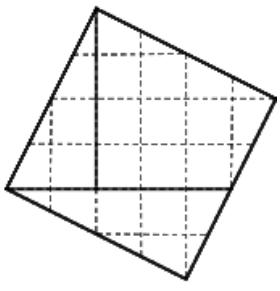


À l'origine, le puzzle était non quadrillé et obtenu à partir du découpage d'un carré en deux triangles et un quadrilatère.

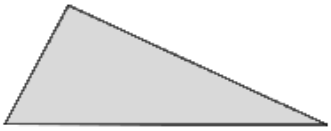
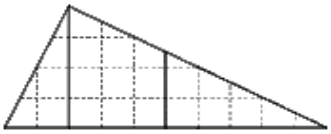


Cette variante quadrillée a été utilisée en atelier dans une classe de **M**oyenne **S**ection – **G**rande **S**ection de Moselle. Le puzzle est formé des trois pièces citées ci-dessus, elles sont obtenues à partir du découpage d'un rectangle : les pièces ne sont pas retournables et des alignements doivent être respectés.

En **M**oyenne et **G**rande **S**ection, l'élève doit recouvrir les gabarits à l'échelle d'un rectangle, d'un carré et d'un triangle (donnés successivement dans cet ordre) avec les trois pièces du puzzle.

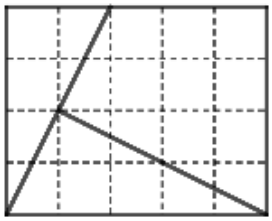
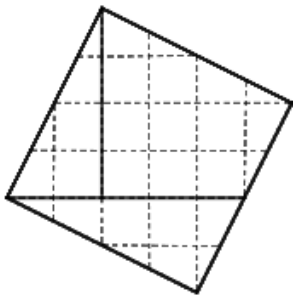
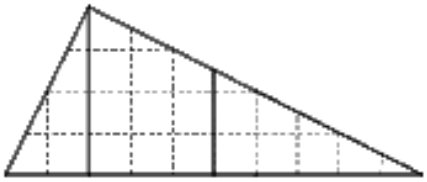
Gabarit	Solution	Remarques
		Les lignes du quadrillage sont parallèles aux bords du rectangle, ce qui constitue une aide pour la plupart des élèves. En posant les questions adéquates, on obtient aisément qu'un rectangle a quatre côtés et que ceux-ci ne sont pas tous pareils.
		Les lignes du quadrillage ne sont plus parallèles aux bords du carré et cette fois c'est une difficulté pour l'élève qui procède par essais-erreurs. On demandera ce qui est pareil que dans le rectangle et ce qui est différent afin d'établir que le carré a quatre côtés et qu'ils sont pareils.

retour au sommaire

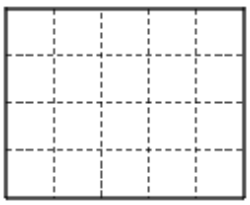
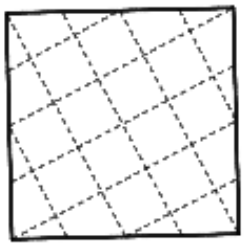
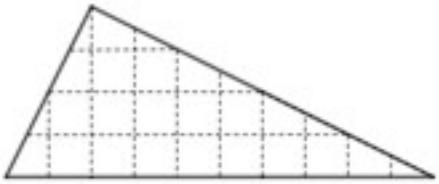
		Les élèves ont tendance à vouloir placer le quadrilatère en premier en bas à gauche, une aide peut être apportée en superposant deux pièces pouvant remplir l'angle de gauche.

En **P**etite **S**ection, on laissera apparente la forme des pièces ou/et le quadrillage dans les gabarits.

La forme des pièces et le quadrillage sont apparents.

Le quadrillage uniquement est apparent.

On pourra faire compter le nombre de côtés de chaque pièce que prendra l'élève.

On dira que s'il y a trois côtés, c'est un triangle et aussi qu'un triangle a trois côtés.
Il y a deux triangles, la troisième pièce a quatre côtés.

retour au sommaire

DANS NOS CLASSES

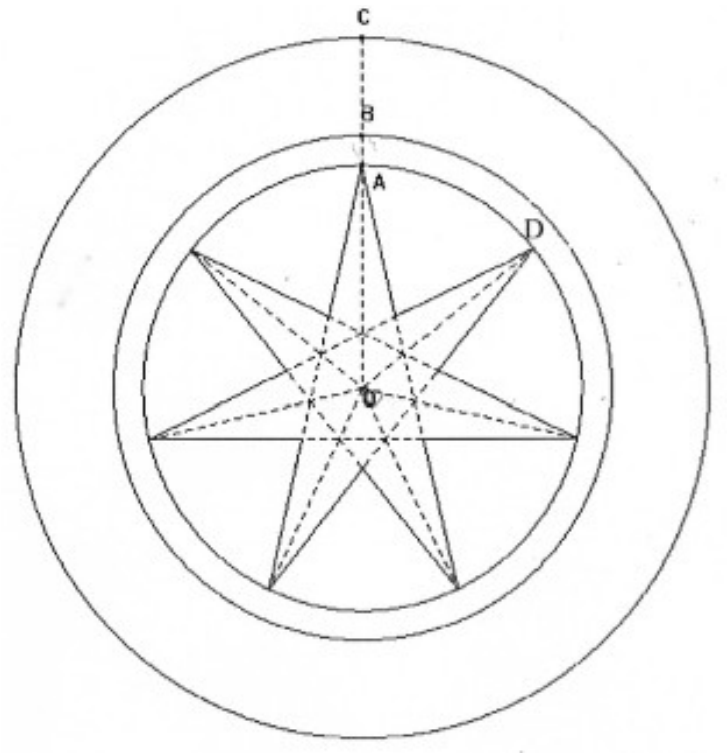
François DROUIN

QUINZE ANNÉES ONT PASSÉ…

Un de nos adhérents m'a envoyé un devoir fait à la maison par sa fille élève de sixième et y a reconnu une figure proposée il y a une quinzaine d'années à mes élèves de sixième dans le cadre d'une classe à projet artistique. Ces activités de dessin d'œils de bœuf avaient par la suite été évoquées dans des moments de formation ; il est intéressant d'en voir leur utilisation actuelle avec les logiciels de géométrie maintenant mis à disposition des élèves.

Le devoir proposé fin 2017

Un œil de bœuf vu à Vignot
(Canton de Commercy – Meuse)



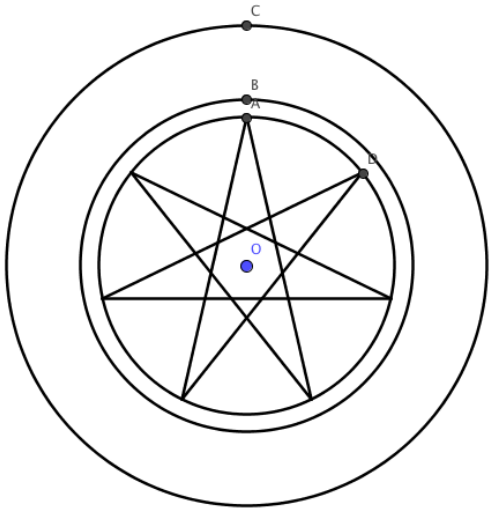
Utilise le logiciel GeoGebra pour tracer la figure.
Il faudra la colorier. Tu peux éventuellement utiliser un autre logiciel en transférant le travail réalisé avec GeoGebra sur ton autre logiciel.

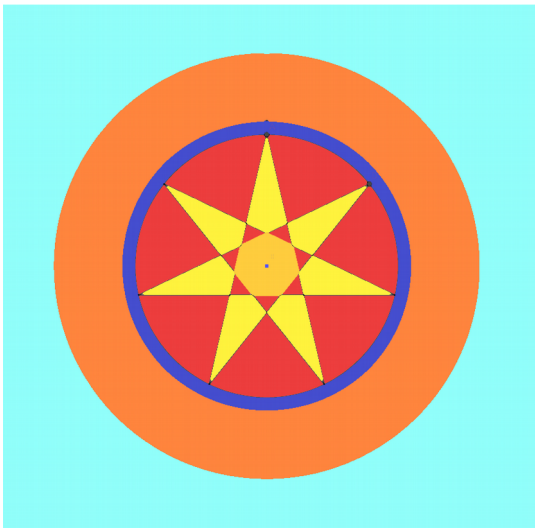
On sait que :
OA = 4,2 cm, OB = 4,7 cm, OC = 6,8 cm et AD = 3,64 cm.
Remarque : le motif admet 7 axes de symétrie.

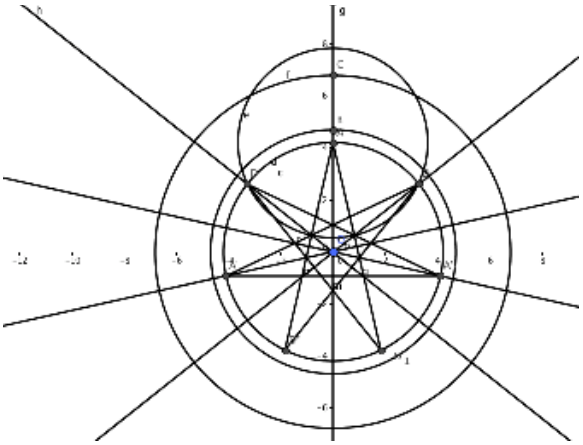
Souviens-toi des consignes données en classe. Tu pourras faire ce travail en plusieurs fois et t'aider d'internet si tu rencontres des difficultés ou me poser des questions en fin d'heure.
Une fois ton travail terminé, dépose le fichier réalisé avec GeoGebra et éventuellement le fichier de la figure coloriée (si tu as utilisé un autre logiciel), dans le casier de collecte « maths » sur l'ENT (pas d'envoi par mail) ;
Forme du nom du fichier : Nom_Prénom_Classe_DM_GeoGebra.
Bon travail.

retour au sommaire

Ce qu'a fourni l'élève

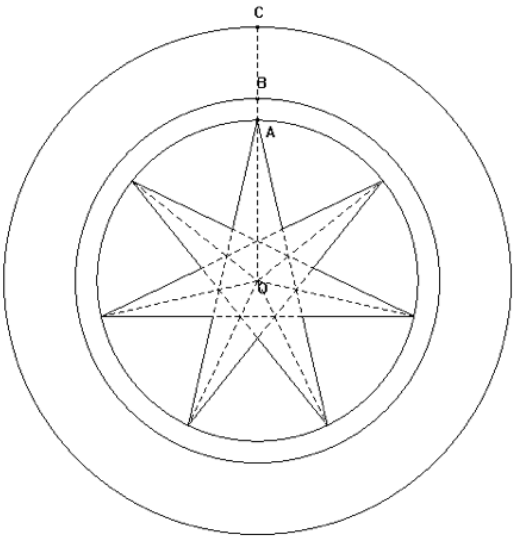






En allant regarder dans la partie protocole du fichier créé, nous remarquons le cercle de centre A et de rayon 3,64 cm permettant d'obtenir deux des sommets de l'étoile.
Ce rayon au dixième de millimètre près figure dans l'énoncé fourni par l'enseignant.

En 2003



Les seules indications étaient :

OA = 4,2 cm, OB = 4,7 cm, OC = 6,8 cm.
Le motif admet 7 axes de symétrie.

Les dimensions indiquées étaient issues de mesures faites sur une photo de l'œil de bœuf. Cette reproduction était affichée dans la classe.

La construction était à faire en utilisant la règle graduée, le compas et le rapporteur.
L'activité était proposée en classe de sixième pendant le troisième trimestre. Elle était l'occasion de se confronter aux reports d'angles de mesure « 360° : 7 » et de constater que suite au dernier report, l'angle restant semblait différent de ceux tracés avec le rapporteur.

« 360° : 7 » était arrondi à 51° ; or 360° - 6×51° = 54°. Le septième angle était plus grand, même si cela n'était pas toujours visible sur les dessins des élèves.

retour au sommaire

L'étude des angles obtenus en tournant autour de O à partir du segment vertical [AB] a été proposée aux élèves. Étaient à calculer le septième de 360°, les deux septièmes de 360°, les trois septièmes de 360°, etc. Les arrondis au degré près fournissent les mesures des angles à reproduire.

De 2003 à 2018

En 2003, la connaissance des axes de symétrie était utilisée pour justifier l'égalité des angles à tracer. L'activité était l'occasion de sortir du domaine géométrique pour travailler les notions d'arrondis et de fraction d'une grandeur.

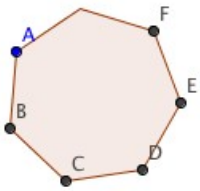
En 2018, la longueur donnée à un dixième de millimètre près peut interpeller mais elle est gérée sans difficulté par le logiciel. La connaissance des axes de symétrie est utilisée pour justifier l'usage du cercle permettant d'obtenir les deux premiers sommets puis de poursuivre le tracé en utilisant l'icône « symétrie orthogonale » du logiciel. L'élève a besoin d'un accès familial à un ordinateur équipé des logiciels nécessaires pour son travail.

Les deux activités ont donc des objectifs différents mais complémentaires. Ce qui était proposé en 2003 peut également l'être en 2018 en utilisant GeoGebra et une feuille de calcul d'un tableur.

Cette photo de l'œil de bœuf permet de se rendre compte qu'il s'agit d'une ouverture dans un mur et que la partie centrale de l'étoile est un vide dans la pierre.

Elle peut inspirer le coloriage demandé à l'élève.

Des élèves plus âgés utiliseront sans doute l'icône « polygone régulier » pour tracer un heptagone puis l'étoile à sept branches.



Quelques compléments

L'heptagone régulier n'est pas constructible à la règle et au compas. Voir Petit Vert n° 127 de décembre 2016 (pages 61 à 65).

Les Petits Verts n°126 (page 80) et n°127 (page 61) abordent des tracés approximatifs peut-être utilisés par les tailleurs de pierre.

https://www.apmep.fr/IMG/pdf/AAA14036.pdf pour les amateurs de tracés d'œils de bœuf octogonaux.

retour au sommaire

DANS NOS CLASSES

DES ZELLIGES EN CLASSE DE TROISIÈME

Claire RENOU, collège Anjou de Sablé-sur-Sarthe

Devoir donné fin septembre 2017

Compétences

	1	2	3	4
M3 Comprendre et utiliser une simulation numérique ou géométrique				
RA3 Démontrer : utiliser un raisonnement logique et des règles établies (propriétés, théorèmes, formules) pour parvenir à une conclusion				
CA1 Calculer de manière exacte ou approchée, en combinant le calcul mental, posé et instrumenté				
CO2 Expliquer à l'oral ou à l'écrit, comprendre les explications d'un autre et argumenter				

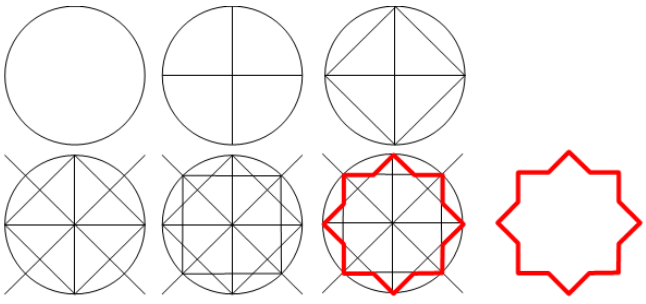
L'art du zellige est apparu au Maroc au Xème siècle et s'est propagé rapidement dans le monde musulman pour devenir l'ornement de base de tout édifice religieux ou privé.
Le zellige est une mosaïque dont les éléments, appelées tesselles, sont des morceaux de carreaux de faïence colorés. Ces morceaux sont découpés un à un et assemblés sur un lit de mortier pour former un assemblage géométrique.
Nous allons travailler sur une partie de mosaïque présente dans l'art du zellige.

Voici deux illustrations de cet art.

L'Alhambra de Grenade

La mosquée de Paris

Les motifs de base des tesselles, s'obtiennent à partir de l'étoile à huit branches, parfois nommé « sceau de Salomon » ou « khatim ».
Dans ce devoir nous allons travailler sur l'étoile à huit branches. Voici sept étapes pour tracer cette étoile :



1. Trace sur une feuille blanche l'étoile à huit branches, à partir d'un cercle de rayon 10 cm.

2. Rédige un programme de construction, étape par étape, de l'étoile à huit branches.

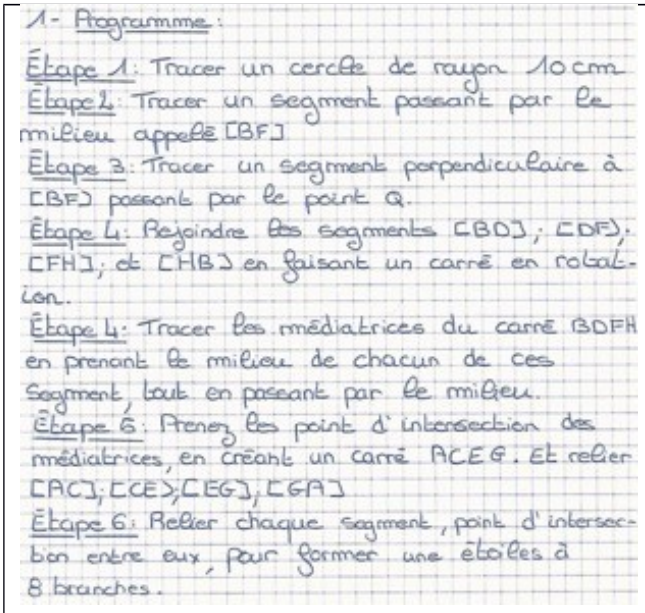
3. On remarque deux quadrilatères entrecroisés sur la figure. Démontre que ce sont des carrés.
4. Trace, si possible, le(s) axe(s) et centre(s) de symétrie de cette étoile.

retour au sommaire

5. Si la figure de départ était le carré ci-contre, quelle transformation du plan nous permettrait d'obtenir le motif de l'étoile à huit branches ? Décrire cette transformation.

6. Calcule le périmètre et l'aire de l'étoile à huit branches.

Quelques productions d'élèves



1- Programme :

Étape 1 : Tracer un cercle de rayon 10 cm

Étape 2 : Tracer un segment passant par le milieu appelé [BF]

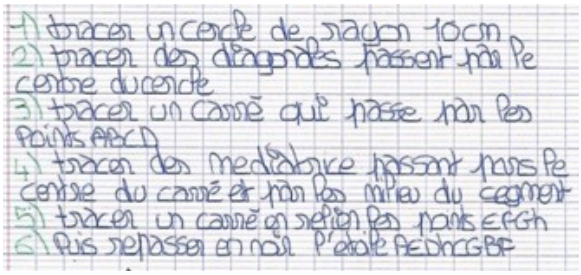
Étape 3 : Tracer un segment perpendiculaire à [BF] passant par le point O.

Étape 4 : Rejoindre les segments [BO] ; [DF] ; [FH] ; et [HB] en faisant un carré en rotation.

Étape 4 : Tracer les médiatrices du carré BDFH en prenant le milieu de chacun de ces segment, tout en passant par le milieu.

Étape 6 : Prenez les point d'intersection des médiatrices, en créant un carré ACEG. Et relier [AC] ; [CE] ; [EG] ; [GA]

Étape 6 : Relier chaque segment, point d'intersection entre eux, pour former une étoiles à 8 branches.



1) tracer un cercle de rayon 10cm
2) tracer des diagonales passant par le centre du cercle
3) tracer un carré qui passe par les points ABCD
4) tracer des médiatrice passant par le centre du carré et par les milieu du segment
5) tracer un carré en reliant les points EFGH
6) Puis repasser en noir l'étoile AEBHCGDF

Ces deux exemples ne permettent la réussite des tracés que si la figure à obtenir est connue du lecteur des textes. Le conseil avait été donné aux élèves de faire tester leurs programmes : des tests faits auprès de personnes étrangères à la classe auraient sans doute montré les failles des écrits, en particulier à propos des points nommés rarement définis. La rédaction de tels programmes de construction n'est pas encore naturelle pour les élèves.

Concernant la question 5, tous n'ont pas retrouvé la rotation et ceux qui y ont pensé ont souvent oublié d'en préciser le sens et l'angle.

Concernant la question 6, une aide a été demandée par les élèves : en début d'une heure de cours, quinze minutes ont été prises pour voir le « découpage » et les longueurs manquantes à calculer à l'aide du théorème de Pythagore.

Devoir donné mi janvier 2018

Compétences

	1	2	3	4
CHER2 : S'engager dans une démarche scientifique, observer, expérimenter, émettre des hypothèses, (Domaines 2, 4)				
CHER3 : Tester, essayer plusieurs pistes de résolution (Domaines 2, 4)				
CHER4 : Décomposer un problème en sous-problèmes (Domaines 2, 4)				
MOD2 : Traduire en langage mathématique une situation réelle (Domaines 1.3, 2, 4)				
REPR4 : Utiliser, des représentations de solides et de situations spatiales (Domaines 5, 1.3)				
RAIS1 : Résoudre des problèmes impliquant des grandeurs variées : mobiliser ses connaissances, exploiter ses erreurs (Domaines 3, 2, 4)				
COMM1 : Faire le lien entre le langage naturel et le langage mathématique (Domaines 3, 1.3, 1.1)				
COMM2 : Expliquer à l'oral ou à l'écrit, comprendre les explications d'un autre et argumenter (Domaines 3, 1.3, 1.1)				

retour au sommaire

En observant bien les mosaïques de l'art zellige, on voit que certaines pièces sont obtenues en modifiant le motif de l'étoile à huit branches. Voici quelques motifs de base utilisés par les artisans.

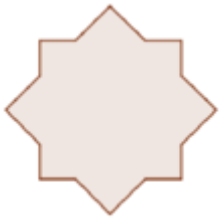


Figure 1

Figure 2

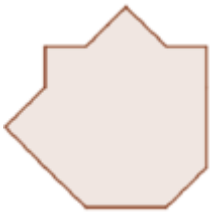


Figure 3

Figure 4

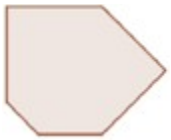


Figure 5

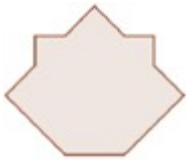


Figure 6

Figure 7

Figure 8

Figure 9

Figure 10

Figure 11

Figure 12

Figure 13

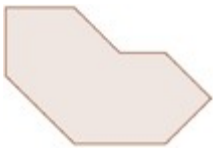
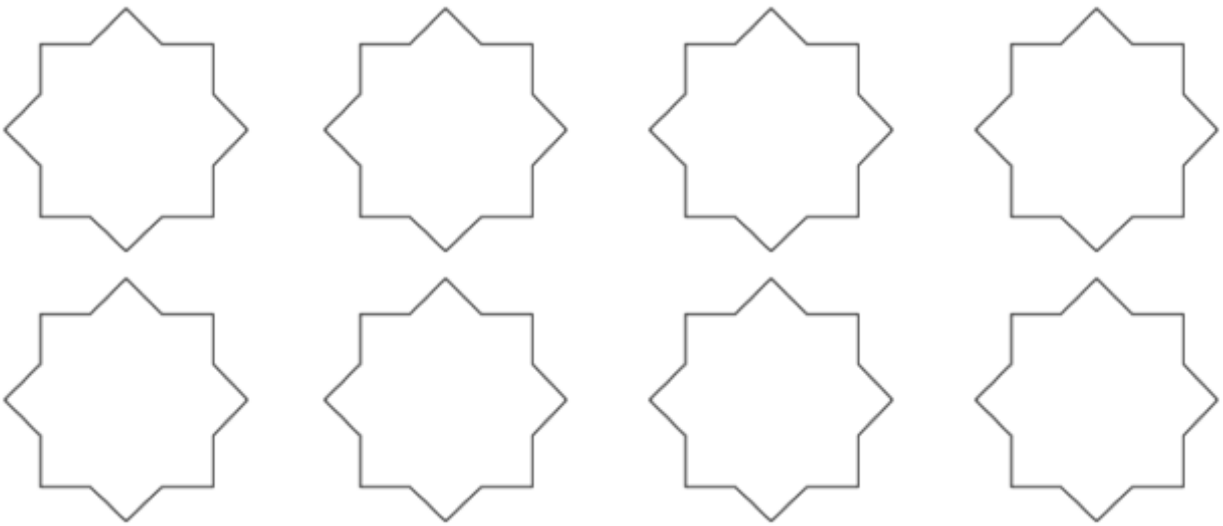
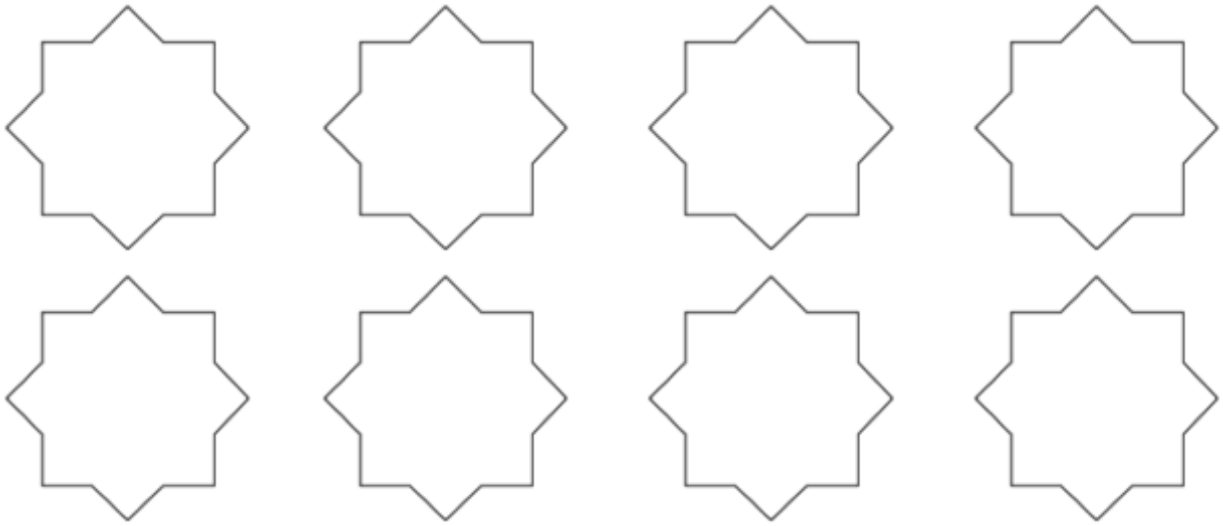


Figure 14

1. Reproduis ci-dessous ces motifs.



retour au sommaire



2. Choisis une des huit pièces dérivées de l'étoile à huit branches et rédige un programme de construction permettant de l'obtenir.
La première étape du programme de construction sera obligatoirement : « Tracer un cercle de centre O et de diamètre AB = 10 cm ». Ton programme peut comporter des croquis ou des dessins afin d'aider à la compréhension.
Astuce : Une fois le programme rédigé, tu peux le faire tester par une personne afin de vérifier qu'il est complet et clair.

À partir de maintenant, nous allons travailler sur le zellige ci-contre:

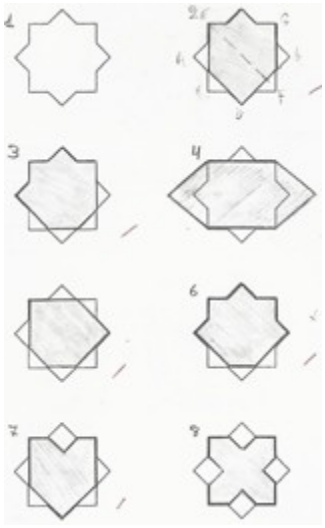
3. Donne les différents types de pièces qui composent ce zellige. Tu peux utiliser les numéros pour les figures présentées au début du sujet et/ou faire un croquis si certaines ne sont pas répertoriées.

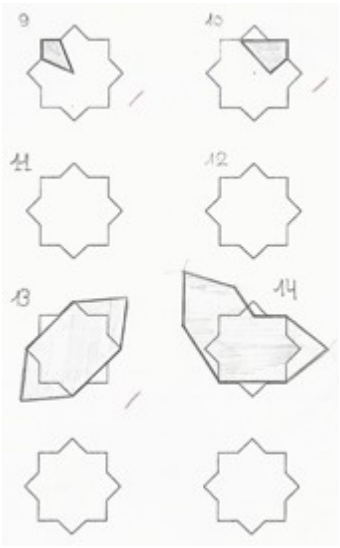
4. Les zelliges sont des pavages du plan qui utilisent les transformations du plan : symétries axiales et centrales, rotations et translations.
a) Trace les axes de symétries du zellige précédent.
b) Quelle est l'image de 1 par la rotation de centre A et d'angle 90° dans le sens horaire (sens des aiguilles d'une montre) ?
c) Quelle est l'image de 3 par la rotation de centre A et d'angle 45° dans le sens anti-horaire ?
d) Quel est l'angle de la rotation de centre C qui transforme 8 en 9 ?
e) Trouve deux rotations, de centre différent, qui transforme 6 en 7.
f) Donne une translation présente sur ce zellige.

5. Sur une feuille petits carreaux, à partir d'un carré de 20 cm sur 20 cm, reproduis le zoom suivant du zellige précédent et colorie le. Laisse visibles les traits de constructions au crayon de papier.

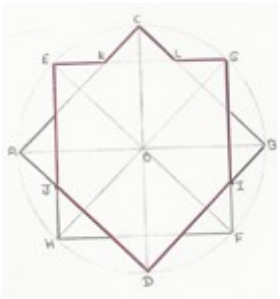
retour au sommaire

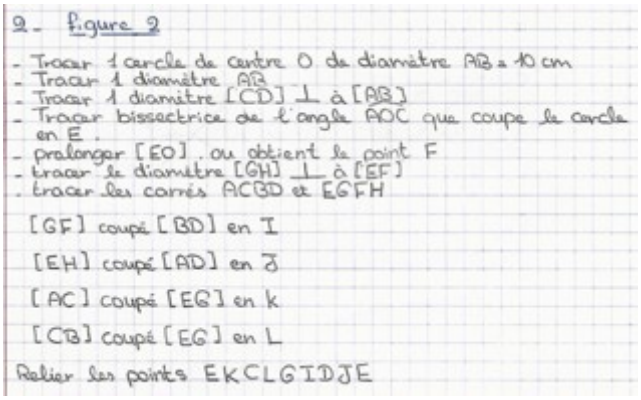
Quelques productions d'élèves.





Les pièces ne sont pas toujours perçues comme pouvant être obtenues à partir de l'étoile à huit branches.





La classe comporte deux élèves syriennes arrivées en France l'an dernier. Ci-dessous se trouve le programme de construction de la pièce 2 écrit par l'une d'entre elles.
Le cercle utilisé pour le tracé de l'étoile à huit branches n'est plus utilisé lors de la reproduction du motif central du zellige. Le quadrillage du papier est sollicité : les pièces de couleur violette ne sont plus superposables.

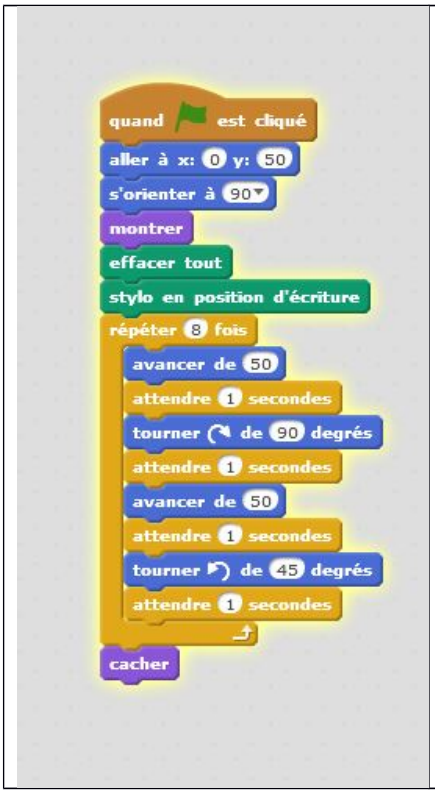
Les sources

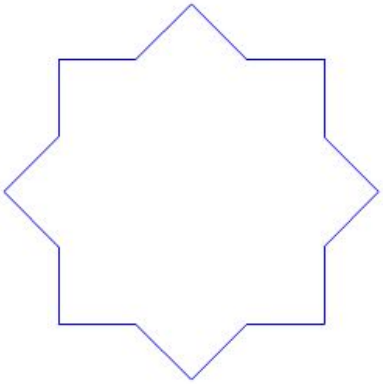
Ont été utilisés pour préparer ce devoir : le travail de Céline Coursimault (PLOT n°20 et brochure « Maths et arts ») , les propositions de Fathi Drissi dans cette même brochure , l'article de Céline Prouteau (l'art du zellige et les azulejos dans la revue n°175 « Chantiers de la régionale Ile de France »), l'article de Julie Benoit (PLOT n°58) à propos des zelliges à la Grande mosquée de Strasbourg, les deux ouvrages d'Éric Broug : celui édité en 2013 a fait l'objet d'une note de lecture dans le PV126 à la page 82.
Afin d'y intégrer les TICE en AP (tous les élèves n'ont pas un ordinateur), une ressource supplémentaire a été trouvée dans le site de l'académie de Créteil: Mathématiques et outils numériques au collège (pages 13 à 19, activité zellige).

Compléments confiés au comité de rédaction

Bien que n'ayant jamais enseigné les mathématiques, une collègue retraitée a repéré une vidéo présentant la réalisation en direct de zelliges. Des gabarits sont utilisés et l'artisan doit être très précis lors des découpes.

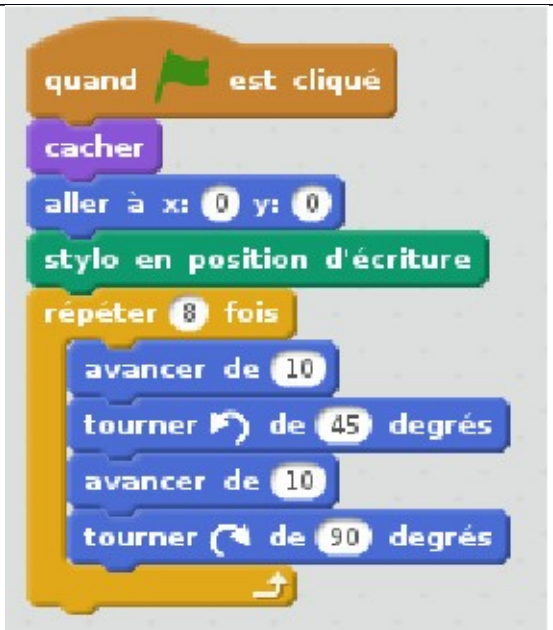
retour au sommaire





Laurent nous a fourni ce programme Scratch ainsi que de quoi suivre son déroulement en direct.

En 2016, dans le cadre d'une formation aux nouveaux programmes de collège, Fathi avait présenté la transformation d'un exercice d'un manuel de cinquième. Le lutin de Scratch est sollicité après une recherche de propriétés géométriques de l'étoile à huit branches.

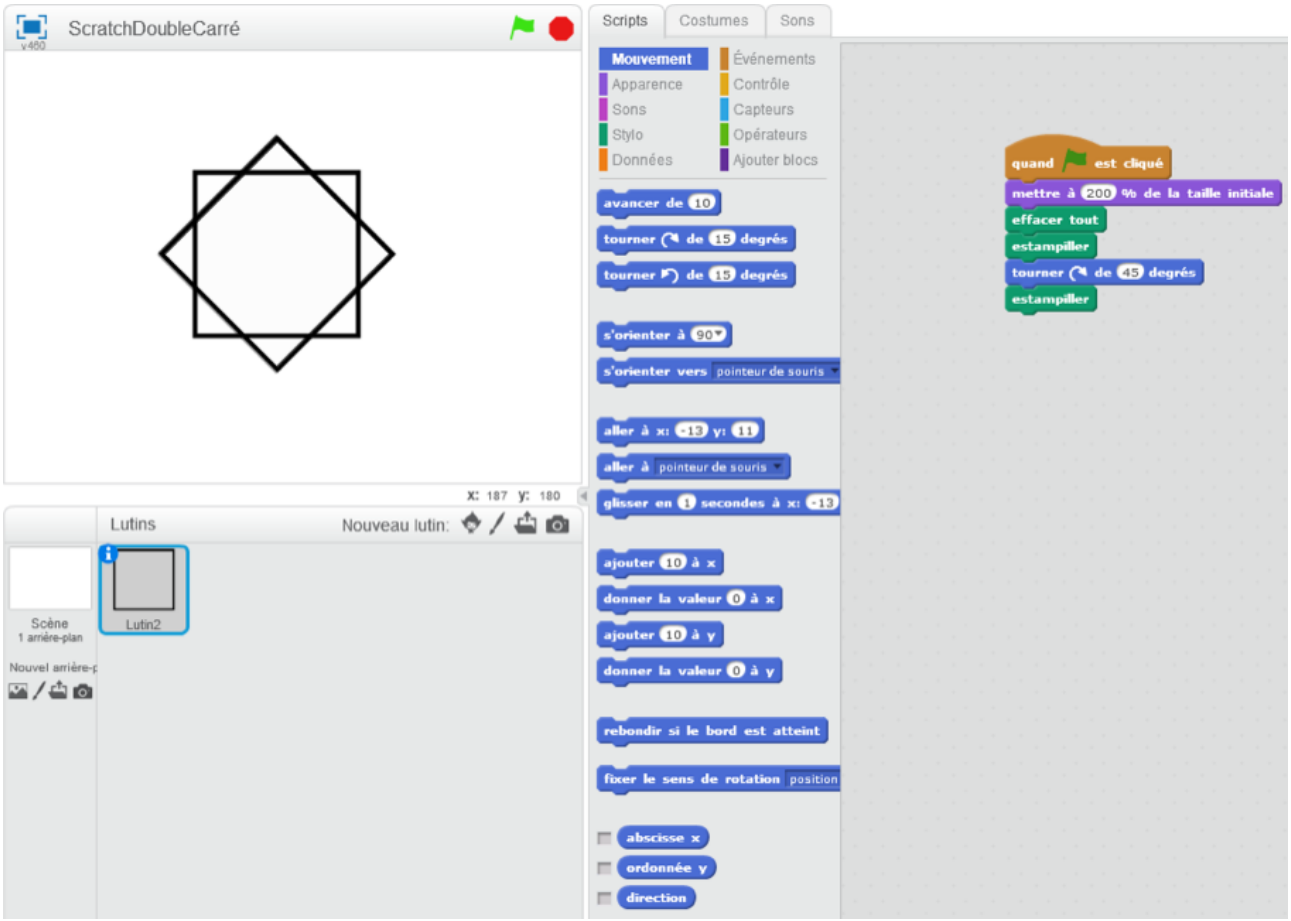


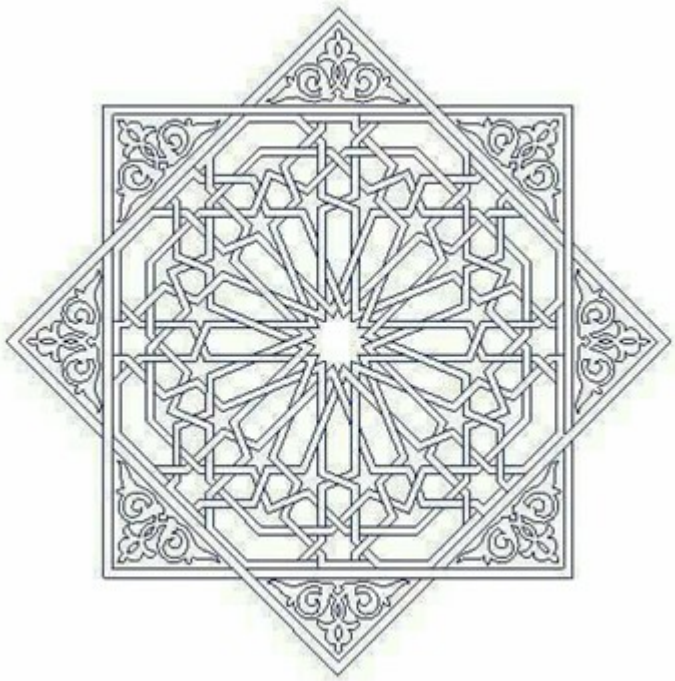
L'étoile à huit branches était l'objet d'un contrôle pour des élèves de Gilles en option ISN.

Michel L s'est intéressé à un script permettant de tracer les deux carrés imbriqués : ceux-ci font apparaître l'étoile à huit branches

retour au sommaire

Sébastien a crée un script montrant comment visualiser l'étoile à huit branches en utilisant une rotation d'un premier carré tracé.





retour au sommaire

DANS NOS CLASSES

RICOCHETS : UNE ACTIVITÉ AVEC LE NUMÉRIQUE

Par Gilles Waehren, lycée Mangin de Sarrebourg

Introduction

Quelques années d'enseignement en BTS SN (Systèmes Numériques) m'ont permis de constater le manque d'aisance de mes anciens élèves de STI 2D SIN (Systèmes d'Information et Numérique) dans l'usage des outils numériques. Le présupposé de connaissances plus avancées dans le domaine, du fait d'enseignements dédiés à l'utilisation d'un ordinateur, peut mener à quelques déconvenues. Recourir à l'informatique pour explorer n'est pas naturel et certains élèves de première année de BTS m'ont déjà rendu des feuilles de calcul remplies de calculs faits « à la main » ! Les sciences physiques ont aussi besoin de ces compétences en tableur et partent du même a priori pour aboutir à la même conclusion : ce n'est pas un acquis.

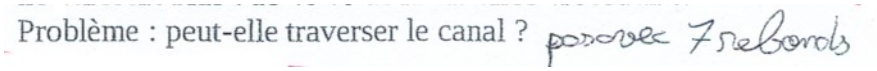
Il n'en subsiste pas moins que le tableur – ou l'algorithmique dans une certaine mesure – pourront intervenir plus souvent qu'on ne se l'imagine dans leur pratique professionnelle ; plus sûrement que GeoGebra ou qu'un logiciel de calcul formel.

Présentation de l'activité

L'objectif de cette activité était donc de motiver l'usage du tableur ou de la calculatrice programmable dans le cadre de la résolution d'un problème lié aux suites géométriques. Je traite toujours ce chapitre en début d'année de Terminale STI2D, car il met tous les élèves en confiance sur un thème qui revient dans presque tous les sujets de baccalauréat. Il permet également d'aborder les problèmes de limites assez naturellement et, bien sûr, de générer, avec des opérations assez simples, une série de valeurs. Je pense que d'autres chapitres pourraient se prêter pas à la mise en place de TP comme celui-ci et cela pourra faire l'objet d'autres articles dans le « Petit Vert ».

Le but du problème était énoncé ainsi :

> *« Un enfant s'amuse aux ricochets sur un canal de 20 mètres de large.*
> *Entre la berge et le premier rebond, la pierre a parcouru 12 mètres. Après chaque rebond, la pierre ne parcourt plus que 40 % de la distance précédente.*
> *Problème : peut-elle traverser le canal ? »*



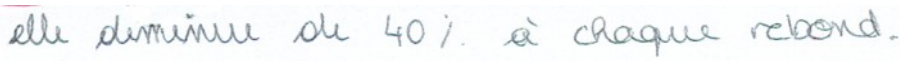
(réponse de Melvyn)

Il s'agissait d'une situation relativement classique. La fiche élève (en annexe) était assez guidée. Je me suis inspiré de l'approche des autres enseignements de cette filière, où certaines séances de TP sont très détaillées pour ne pas multiplier les difficultés. Les questions alternaient restitution de connaissances du cours nécessaires aux formules sur tableur ou calculatrice et manipulations effectives. J'avais également prévu comme aides (assez peu utilisées) une copie d'écran de la feuille de calcul ainsi que le deuxième algorithme, à traduire. Des questions de recherche sur le pourcentage d'évolution ont été traitées par l'un ou l'autre élève plus rapide. L'évaluation du travail a donné lieu à une note sur 10 sur des critères de réussite par question plutôt binaires, en valorisant tout particulièrement le travail informatique. On pourra réfléchir à une évaluation par compétence, plus pertinente.
Le travail devait se faire en une heure. La salle informatique est de toutes façons attribuée à la classe sur un des créneaux de cours.

retour au sommaire

Travaux des élèves sur les connaissances générales

« Que peut-on dire de la suite des distances entre deux rebonds ? »
Réponse :



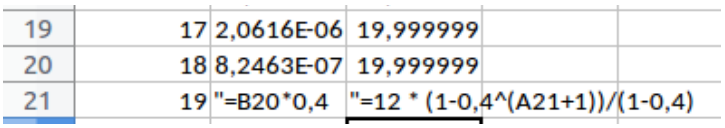
(Charlotte, bonne élève)

Il est vrai que l'intitulé « Que peut-on dire … ? » donne souvent lieu à des réponses très variées. Cependant, les formulations au bac, telles que « Quel type de suite … ? », sont peu pertinentes, du fait qu'il n'y a que deux types de suites au programme de STI2D : les géométriques et les non géométriques ! J'attendais ici le résultat d'une lecture réfléchie de l'énoncé, et si beaucoup ont identifié une suite géométrique de raison 0,4 et de premier terme 12, nécessaire pour construire la première liste de valeurs sur tableur, le taux de 40 % a quelquefois été perçu comme un taux de diminution (« la raison est 0,6 »). J'ai aussi vu le premier terme égal à 20 (la largeur du canal). Cette phase d'extraction de l'information n'était pas censée être difficile, mais il a fallu vérifier avec certains élèves que les notions du cours (raison, premier terme) avaient bien été repérées dans le texte.

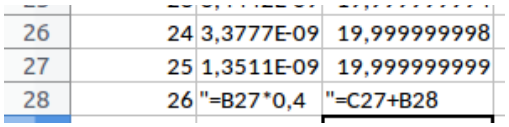
La question « Comment calculer … ? » pouvait laisser une certaine place à l'interprétation. Penser à la formule de la somme de termes de suite géométrique ne s'est pas fait immédiatement. Ici aussi, ce type de travail, plus ouvert qu'une séance d'exercices, est l'occasion pour les élèves de chercher à répondre sans recourir aux méthodes vues en classe. Il n'était pas nécessaire d'utiliser cette formule pour déterminer les valeurs cherchées, mais beaucoup ont remarqué qu'elle simplifiait le premier algorithme (voir ci-après). Enfin, ce fut aussi l'occasion de retrouver la bonne expression dans le cours – et ne pas la confondre avec celle du terme général ou avec la relation de récurrence – mais aussi d'insister sur la numérisation en remplaçant les termes de l'expression par leur valeur afin de repérer la variable : le nombre de termes.

Travaux des élèves sur le tableur

À l'aide de la relation de récurrence, les élèves ont pu écrire la formule tableur nécessaire à la construction de la suite des distances. Cette étape s'est faite sans encombre. Par contre, l'écriture de la longueur totale a demandé plus de temps. Je voulais qu'ils réfléchissent à la façon dont on peut effectivement calculer la somme des termes d'une suite. C'est un exercice qui n'est pas nécessairement évident pour qui ne l'a pas vu au moins une fois. On a donc commencé avec l'exemple « 1+2+3+4+5 » pour se rendre compte du mécanisme. Ce travail de décomposition du calcul sans chercher à utiliser une quelconque astuce est assez formateur pour l'écriture d'algorithme : il s'agit de se regarder calculer pour savoir ce que l'on va pouvoir demander à la machine. Ici, il fallait voir qu'à chaque nouveau terme de la somme, on utilisait la somme des précédents pour effectuer une seule addition à la fois (copie d'écran de droite). Bien entendu, une bonne formule bien comprise donne le même résultat (copie d'écran de gauche) ; mais, les termes de la suite ne sont plus nécessaires au calcul de la somme.



19	17	2,0616E-06	19,999999
20	18	8,2463E-07	19,999999
21	19	"=B20*0,4	"=12 * (1-0,4^(A21+1))/(1-0,4)



26	24	3,3777E-09	19,999999998
27	25	1,3511E-09	19,999999999
28	26	"=B27*0,4	"=C27+B28

Le calcul de puissances reste une opération lourde pour un ordinateur, source d'erreurs notamment sur les décimaux, même si les résultats apparaissent instantanément. J'essaie de rendre les élèves de STI 2D sensibles à ce genre de problème pour motiver des formules comme celles de la copie d'écran de droite. On trouve sur ces deux exemples de sommes, deux conceptions de la programmation en STI 2D : à gauche, la programmation par positionnement de variables, pratique assez courante dans leur enseignement SIN pour la gestion des cartes type Arduino ; à droite, une programmation plus algorithmique où l'on

retour au sommaire

cherche à simplifier les opérations, approche plus conforme à notre sensibilité mathématique. On retrouvera cette différence dans le traitement des algorithmes sur calculatrice.

Les élèves de STI2D manipulent tous les jours de nombreuses expressions, parfois compliquées, et ne sont pas effrayés par celles qui leur sont proposées en mathématiques. Elles sont cependant, pour certaines, difficiles à mémoriser, et c'est aussi dans cette filière qu'on va trouver des élèves à la recherche de solutions de contournement efficaces. Malgré cela, il a fallu corriger de nombreuses formules pour obtenir le résultat voulu.

Les deux questions qui suivaient avaient pour but d'exploiter les résultats du tableur. Le record de l'enfant étant établi à 7 ricochets, la moitié des élèves a limité son tableur au rang 7 (voir ci-dessous) . Il se trouve que cela suffisait pour obtenir les 95 % et 99 % demandés, mais comment le savoir a priori ? On pourra ici modifier le pourcentage inciter les élèves à poursuivre leur investigation.

	A	B	C
1	nbr de rebonds	distance rbd	longueur totale parcourue
2	0	12	12
3	1	4,8	16,8
4	2	1,92	18,72
5	3	0,768	19,488
6	4	0,3072	19,7952
7	5	0,12288	19,91808
8	6	0,049152	19,967232
9	7	0,0196608	19,9868928

Certains élèves ont cherché à justifier leurs réponses en recopiant toutes les valeurs du tableur, rebonds par rebonds, d'autres ont mis en évidence les valeurs sur la feuille de calcul (voir exemple ci-dessous). Mais les avis étaient partagés sur le nombre de rebonds à effectuer pour 95 % et pour 99 % de la largeur : 3 et 5 rebonds contre 4 et 6 rebonds (ci-dessous : l'élève a commencé sa suite à u_1).

	A	B	C	D	E	F	G	H	I
1	Rebond	Distance		Somme de terme		Raison			
2	1	12		12		0,4			7 Premier rebonds
3	2	4,8		16,8					
4	3	1,92		18,72					
5	4	0,768		19,488					95% du canal
6	5	0,3072		19,7952					
7	6	0,12288		19,91808					
8	7	0,049152		19,967232					99% du canal
9	8	0,0196608		19,9868928					
10	9	0,0078643		19,99475712					
11	10	0,0031457		19,997902848					

Rien n'empêche d'initialiser la suite au rang 1 plutôt qu'au rang 0, mais il peut être bon d'insister sur la formulation de la conclusion. L'intitulé de la question laissait peu de place à des réponses différentes.

Ce premier travail sur tableur fut l'occasion de constater que nous ne consacrons pas suffisamment de temps à l'exploration sur ce formidable outil de calcul. C'est pourtant, on le voit ici, l'occasion de manipuler des expressions algébriques complexes et de donner du sens aux calculs. Les réflexions menées devaient permettre de construire plus facilement les programmes calculatrices de la deuxième partie du TP.

L'un ou l'autre élève a demandé à me rendre le travail plus tard pour traiter la dernière partie :

	A	B	C	D	E	F	G	H	I	J	K
1	NB REBOND	LONG TOTAL	DIST REB								
2	0	12	12			13	13			11	11
3	1	4,8	16,8			4,55	17,55			4,95	15,95
4	2	1,92	18,72			1,5925	19,1425			2,2275	18,1775
5	3	0,768	19,488			0,557375	19,699875			1,002375	19,179875
6	4	0,3072	19,7952			0,1950813	19,894956			0,4510688	19,630944

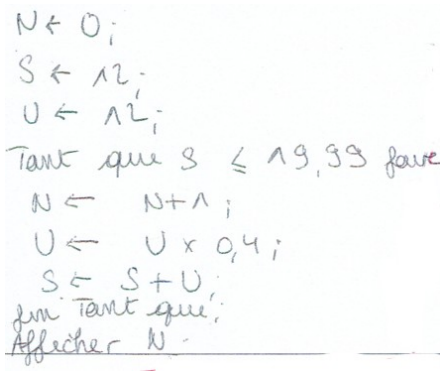
Travaux des élèves sur la calculatrice

Pour cette partie, plus constructive, certains élèves ont manqué de temps. Le premier programme, qui demandait la somme des termes, a été assez rapidement écrit ; mais il fallait

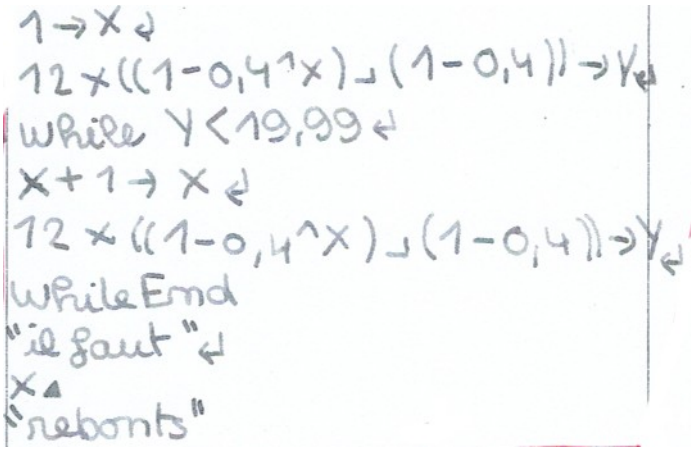
retour au sommaire

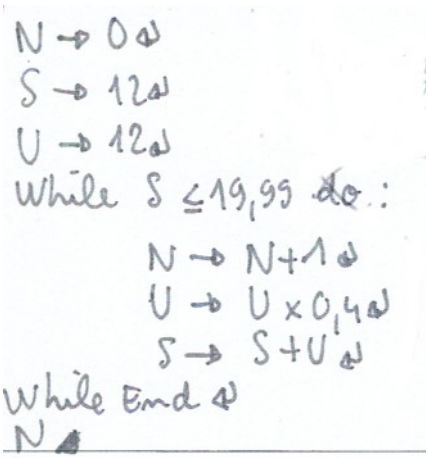
tout de même l'implémenter. La calculatrice n'est pas le meilleur support pour ce genre de travail, mais c'est le seul dont ils disposent à l'examen. Ayant déjà vu des élèves écrire des programmes pendant l'épreuve de mathématiques, je m'étais dit qu'il était intéressant qu'ils apprennent à le faire pour traiter les questions d'algorithmique, récurrentes dans les sujets actuels.

Comme les appuis que je fournissais donnaient l'algorithme, j'ai demandé à ce que les élèves recopient leurs programmes sur le document élève, ne pouvant pas ramasser toutes les calculatrices. Certains se sont contentés de recopier – voire de coller directement - l'algorithme fourni sans chercher à le traduire ; les petites aides sont parfois à double tranchant (voir ci-contre). J'ai fait remarquer à ces élèves, sur leur copie, que j'attendais un programme. La différence n'est pas toujours très claire, dans leur esprit, entre programme et algorithme.



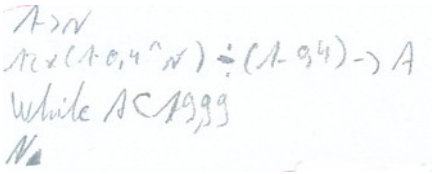
Ce deuxième programme est un classique problème de seuil, relativement courant à l'examen. Comme sur tableur, on retrouve ici les deux approches du calcul de la somme. La condition de boucle est une inégalité stricte à gauche et large à droite : dans la situation présente, cela n'avait que peu d'importance. Les deux programmes sont écrits en langage CASIO (matériel recommandé dans mon Lycée). On remarquera à droite une transcription moins fidèle (positionnement des flèches) ; il s'agit vraisemblablement d'une réécriture de l'algorithme, car ce programme ne peut pas fonctionner sur CASIO. Nota Bene : cette orientation de la flèche sur les calculatrices est peu conforme aux nouvelles instructions du B.O. quant à la notation de l'affectation de variables.



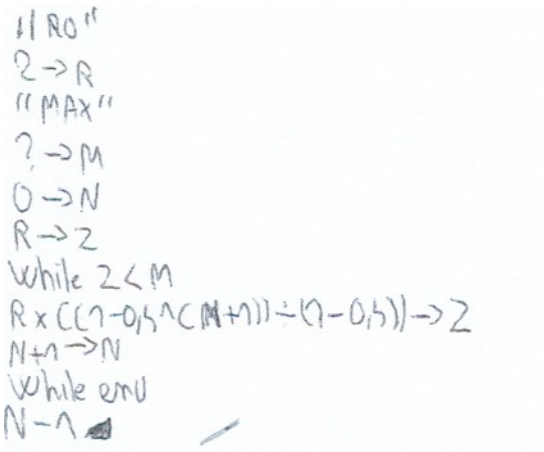


retour au sommaire

Exemple 1 :



Exemple 2 :



J'ai également obtenu quelques productions plus personnelles. Dans l'exemple 1, le corps de boucle est totalement absent, mais l'initialisation est correcte, la condition de boucle est bien écrite et l'élève a vu que l'information attendue était la valeur du rang. L'une des réussites de cette séance reste l'identification de la boucle « Tant que » comme clé de l'algorithme. On peut penser que l'élève n'a probablement pas eu le temps de tester son programme pour le corriger, puisque la boucle est ici infinie.

Le deuxième exemple relève déjà d'une certaine expertise, puisque l'élève demande la saisie du premier terme et du seuil et qu'il affiche le rang diminué de 1 (il est augmenté avant de sortir de la boucle). Une inversion des deux instructions de la boucle aurait été plus efficace.

Bilan

Les élèves ont été relativement actifs lors de cette séance puisqu'ils pouvaient fonctionner comme dans les TP de SIN ou de Sciences Physiques : manipuler, tester, circuler, demander de l'aide aux camarades ou au professeur. Leur manque d'aisance avec le tableur ou avec l'algorithmique ne les ont pas empêchés d'utiliser volontiers l'ordinateur ou la calculatrice. Les freins à la réussite étaient plutôt situés au niveau des connaissances à mobiliser.

Pour améliorer ce TP, on pourra modifier certaines valeurs de l'énoncé pour éviter des résultats trop évidents : taux de diminution, formulation de certaines questions, pourcentage de largeur du canal à atteindre. Les questions d'ouverture méritent d'être remaniées pour pouvoir jouer plus facilement sur la raison et le premier terme de la suite.

Les incitations à l'usage des outils numériques sont nombreuses dans les programmes de mathématiques de toutes les filières. On trouve un grand nombre d'activités numériques sur Internet, mais il n'est pas toujours aisé de construire une séance où l'ordinateur, la calculatrice, va apporter une véritable plus-value par rapport à un travail d'entraînement sur exercices. Les séances informatiques sont une chance pour les élèves des séries technologiques de montrer des compétences qui ne se limitent pas à la production d'un écrit. Mais, il n'est pas commode d'accepter de sacrifier de précieuses heures pour enrichir tel ou tel chapitre dont le contenu notionnel est déjà difficilement accessible. On pourra se focaliser sur des chapitres plus faciles pour donner à nos élèves l'habitude d'une utilisation pertinente d'outils sur lesquels, ils manquent, contrairement à certains clichés, de plus en plus d'autonomie et de savoir-faire.

retour au sommaire

Annexe : l'énoncé proposé aux élèves

Un enfant s'amuse aux ricochets sur un étang qui mesure 30 mètres dans sa plus grande longueur.
Entre la berge et le premier rebond, la pierre a parcouru 12 mètres. Après chaque rebond, la pierre ne parcourt plus que 60 % de la distance précédente.
Problème : peut-elle traverser le canal ?

Que peut-on dire de la suite des distances entre deux rebonds ?
Réponse :

Sur tableur : (déposer le fichier dans le casier de collecte de l'ENT)

- afficher le numéro des rebonds, les distances entre deux rebonds consécutifs, la longueur totale parcourue par la pierre.

Le record de cet enfant est 7 ricochets : quelle est alors la distance parcourue par sa pierre ?
Réponse :

Au bout de combien de rebonds, la pierre a parcouru 95 % de la largeur du canal ?
Même question avec 99 % de la largeur.
Réponses :

Comment calculer la distance totale parcourue par la pierre ?
Réponse :

Sur calculatrice :

- écrire un programme qui, selon le nombre de rebonds entré, donne la longueur totale parcourue ;
- écrire un programme qui permet de connaître le nombre de rebonds nécessaires pour une longueur totale de 29,99 mètres.

Recopier les programmes dans les cadres ci-dessous :

Programme 1	Programme 2

Pour aller plus loin :
Supposons que la plus grande longueur de l'étang soit 40 m. Comment choisir la distance avant le premier rebond pour traverser l'étang en 7 ricochets ?

RÉPONSE :

retour au sommaire

ÉTUDE MATHÉMATIQUE

ÉLÉMENTS DE CRYPTOGRAPHIE ARITHMÉTIQUE

Par Alain SATABIN, professeur honoraire

Sommaire de l'article :

1. CHIFFREMENT À CLÉ RÉVÉLÉE

Nous examinons ici quelques procédés de chiffrement utilisant un calcul arithmétique. Les textes sont supposés ne contenir que des lettres non accentuées (aucun chiffre, ni ponctuation, ni espace). Chaque lettre est identifiée à un nombre compris entre 0 et 25 (du A au Z) :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Les procédés peuvent évidemment s'étendre à un jeu de caractères plus complet en adaptant les fonctions arithmétiques utilisées.

1.1. Chiffre de César (– 101 / – 44)

Il s'agit là d'un simple glissement de l'alphabet. Chaque lettre est remplacée par sa translatée d'une certaine constante dans l'alphabet bouclé (du Z, on revient au A).

La fonction arithmétique correspondante est donc du type $n \longrightarrow n+k\ [26]$. Le déchiffrement consiste évidemment à appliquer l'opération $n \longrightarrow n\text{-}k\ [26]$.

Par exemple, avec $k = 15$, le texte **BONJOUR** se chiffre **QDCYDJB** ; et avec $k = 7$, **ZHSBA** se déchiffre **SALUT**.

Ce type de fonction peut être affine du type $n \longrightarrow pxq\ [26]$ où p est premier avec 26 afin de posséder un inverse p' dans z / 26z. Sa réciproque, permettant le déchiffrement, est alors $n \longrightarrow p'x(n\text{-}q)\ [26]$.

Par exemple, avec $k = 15$, le texte **BONJOUR** se chiffre **QDCYDJB** ; et avec $k = 7$, **ZHSBA** se déchiffre **SALUT**.

Pour sa part, César utilisait une constante égale à 3 et l'alphabet latin ne comportait que 20 lettres. Le fait qu'il n'existe que 25 chiffres de César rend ce procédé extrêmement vulnérable !

1.2. Chiffre de substitution

Dans ce procédé, chaque lettre est remplacée par une autre lettre. Cette permutation de l'alphabet constitue la clé de chiffrement et doit évidemment être convenue entre émetteur et récepteur. Ce mélange peut provenir tout simplement d'une succession des 26 lettres mélangées, ou d'un mélange issu d'un mot clé, ou encore d'une fonction arithmétique bijective de $\mathbb{Z}$ /n $\mathbb{Z}$ dans lui-même.

Ce type de fonction peut être affine du type $n \longrightarrow pxq\ [26]$ où p est premier avec 26 afin de posséder un inverse p' dans z / 26z. Sa réciproque, permettant le déchiffrement, est alors $n \longrightarrow p'x(n\text{-}q)\ [26]$.

En prenant par exemple $p = 5$ et $q = 17$ (donc $p' = 21$), la correspondance mono-alphabétique est :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
R W B G L Q V A F K P U Z E J O T Y D I N S X C H M

et **BONJOUR** se chiffre **WJEKJNY**, alors que **DRUNI** se déchiffre **SALUT**.

retour au sommaire

1.3. Chiffre de Vigénère (1523 - 1596)

Les chiffres de substitution mono-alphabétique ont l'inconvénient de toujours remplacer une même lettre par un même lettre, ce qui les rend vulnérables et facilement cassables par l'analyse des fréquences des lettres du texte chiffré.
Vigénère pallia cet inconvénient en introduisant un mot clé qui, écrit de façon cyclique sous le texte clair, donne, pour chaque lettre, le décalage à lui faire subir (au sens *Chiffre de César*).
Si, par exemple, la lettre **D** du texte clair se trouve associé à la lettre **O** de la clé, la lettre **D** sera chiffrée en utilisant un procédé de César où la lettre **A** est remplacée par un **O** … et donc le **D** par un **R**. Cela revient dans ce cas à décaler l'alphabet de 14 lettres.
Voici un exemple où la clé de chiffrement est **SOL** (qui ne connait pas la clé de sol ?) :

Texte clair	**A**	**D**	**E**	**M**	**A**	**I**	**N**
Clé	S	O	L	S	O	L	S
Décalage	18	14	11	18	14	11	18
Texte chiffré	**S**	**R**	**P**	**E**	**O**	**T**	**F**

La fonction arithmétique de chiffrement est du type $n \longrightarrow n - q \times k_{clef}\ [26]$ où k évolue en fonction de la position du caractère n dans le texte clair.

BONJOUR TOUT LE MONDE avec la clé **VOUTE** se chiffre **WCHCSPFNHYOZYFSI** et le déchiffrement de **UHLGISXVUE** avec la clé **CHAMPS** donne **SALUT A VOUS**.

On voit sur ces exemples qu'une même lettre n'est pas toujours chiffrée de la même façon … à condition de ne pas retomber en face de la même lettre du mot clé. Le risque sera d'autant plus faible que le mot clé est long. Il est d'ailleurs possible de prendre comme mot clé un proverbe ou un texte classique, et le procédé devient incassable si la clé est un texte de même longueur que le texte clair.

1.4. Chiffre de Jefferson (1743 - 1826)

Les procédés de chiffrement utilisés par le président américain Jefferson étaient des variantes du chiffre de Vigénère dans lequel étaient introduits des coefficients multiplicatifs.
Le premier s'appuyait sur la fonction arithmétique de chiffrement du type $n \longrightarrow n + q \times k_{clef}\ [26]$.
Par exemple, avec le mot clé **PLATE** et $q = 11$, le texte clair **BONJOUR** se chiffre de la façon suivante en **KFNKGDI** :

Texte clair	**B**	**O**	**N**	**J**	**O**	**U**	**R**
n	1	14	13	9	14	20	17
clé	P	L	A	T	E	P	L
$k_{clé}$	15	11	0	19	4	15	11
$n + 11 \times k_{clé}$	10	5	13	10	6	3	8
Texte chiffré	**K**	**F**	**N**	**K**	**G**	**D**	**I**

Le déchiffrement utilise évidemment la fonction $n \longrightarrow n - q \times k_{clef}\ [26]$.
Par exemple, toujours avec la clé (**PLATE**;11), **BRLVLJKIPFB** signifie **SALUTATIONS**.
Le second procédé utilisé par Jefferson correspondait à la fonction $n \longrightarrow n + q \times k_{clef}\ [26]$ où p était premier avec 26 pour pouvoir posséder un inverse p' modulo 26 et le déchiffrement se faisait grâce à la fonction $n \longrightarrow p' \times (n - k_{clef})\ [26]$.
Par exemple, avec le mot clé **DEHUIT** et $p = 11$ (et donc $p' = 19$)), **BONJOUR** se chiffre **OCUPGFI** et **TEYGJTEOFHY** signifie **SALUTATIONS**.

retour au sommaire

1.5. Généralisation

Tous les procédés analysés jusqu'ici ne sont que des cas particuliers de la fonction de chiffrement

$$n \in \mathbb{Z}/26\mathbb{Z} \rightarrow p \times n + q \times k_{clef}\,[26]\; p \wedge 26 = 1$$

dont la fonction de déchiffrement est :

$$n \in \mathbb{Z}/26\mathbb{Z} \rightarrow p' \times (n - q \times k_{clef})\,[26]\; p \times p' = 1\,[26]$$

pour lesquels la clé de chiffrement est le triplet (*motclef ; p; q*).
Par exemple, avec la clé (**OPATRE**;7;12), l'inverse de 7 modulo 26 étant 15, **BONJOUR** se chiffre **TSNFQGB** et **IYZEZWPCUHS** signifie **SALUTATIONS**.
On notera les cas particuliers :

- si la clé est du type (B ; 1 ; *k*), c'est un chiffre de César
- si la clé est du type (B ; *p* ; *q)*, c'est un chiffre affine
- si la clé est du type (*mot clef* ; 1 ; 1), c'est un chiffre de Vigénère
- si la clé est du type (*mot clef* ; 1 ; *q*), c'est un chiffre de Jefferson type 1
- si la clé est du type (*mot clef* ; *p* ; 1), c'est un chiffre de Jefferson type 21.6. Le chiffre MIAS

Ce procédé consiste à multiplier modulo 26 le caractère clair par le caractère clé :
$n \longrightarrow n + q \times k_{clef}\,[26]$.
On voit tout de suite l'inconvénient : avec la clé **MATITE**, le texte **A DEMAIN MATIN** devient **AAYSAGAAAWWA** et le déchiffrement pose un réel problème. Par ailleurs, un **A** est toujours chiffré par un **A** avec ce procédé.
Pour pouvoir déchiffrer, il faudrait que chaque caractère du mot clé soit de rang premier avec 26, ce qui ne laisse que 12 lettres possibles … dont aucune voyelle !
Pour pallier cet inconvénient, on peut étendre le jeu de caractères à 37 (nombre premier) en y adjoignant les chiffres et l'espace :

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
J	K	L	M	N	P	P	Q	R	S	T	U	V	W	X	Y	Z	-	
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	

Seul le caractère **0** n'est plus inversible et est interdit dans le mot clé.
Le chiffrement est alors la fonction $n \longrightarrow n + q \times k_{clef}\,[37]$
et le déchiffrement $n \longrightarrow n + (q \times k_{clef})^{-1}\,[37]$ où l'inverse est évidemment considéré modulo 37.
Par exemple, les caractères du mot clé **MATITE** ont pour rangs 22/10/29/18/29/14 et leurs inverses modulo 37 sont respectivement 32/26/23/35/23/8. Déchiffrer un message crypté avec la clé **MATITE** revient à le chiffrer avec la clé **WQNZN8**.
Ainsi, toujours avec la clé **MATITE**, le texte clair **A DEMAIN 8H** se chiffre **ZR7U9TQ88XC**, et le texte crypté **WPJ4U F6CIY** se déchiffre **PLUTOT 8H15**.

2. LE PROBLÈME DE LA TRANSMISSION DES CLÉS

2.1. Le talon d'Achille

La puissance grandissante de l'outil informatique fournit des moyens efficaces aux briseurs de chiffre. Les procédés examinés dans le paragraphe précédent sont loin d'être infaillibles … et sont même brisés, pourvu que le cryptanalyste possède un texte chiffré assez long.

retour au sommaire

Les mêmes moyens informatiques ont offert aux développeurs la possibilité de mettre au point des procédés de chiffrement à clé secrète de plus en plus sophistiqués et qui, eux, résistent aux briseurs les plus tenaces.

Citons pour mémoire le procédé Lucifer, développé chez IBM par Horst Feistel dans les années 70, qui crypte les messages par brouillages itérés. Chaque caractère du texte est remplacé par l'octet correspondant à son code ASCII (de 0 à 255). Cette succession de 1 et de 0 (des bits) est ensuite mélangée par application à chaque bloc de 32 bits de permutations successives. Le battage de ce jeu de cartes repose sur un nombre clé dont la connaissance permettra au récepteur de retrouver l'ordre originel, et donc le texte clair. La fiabilité et l'inviolabilité de ce procédé en fit un standard adopté officiellement aux États-Unis en 1976, sous le nom de DES (*Data Encryption System*). Il demeure encore aujourd'hui une norme américaine de chiffrement pour les échanges commerciaux.

Mais tous ces procédés de chiffrement ont en commun un inconvénient majeur : une clé secrète. Le problème de sa transmission entre les personnes utilisant le procédé est sérieux. Aussi sophistiqué soit-il, un chiffre ne présente plus aucun intérêt si l'ennemi intercepte sa clé.

2.2. Naissance d'un remède

En 1976, Whitfield Diffie et Martin Hellman eurent l'idée de résoudre le problème d'échange des clés grâce à une fonction arithmétique impossible à inverser dans un temps raisonnable.

Il s'agit des fonctions du type $n \longrightarrow a^n \ [p]$ où p est un nombre premier et a un entier différent de 0 et de 1.

Prenons par exemple $a = 53$ et $p = 21\,997\,783$. Sur mon ordinateur, un programme a mis $1{,}3 \times 10^{-4}$ seconde seconde à calculer $a^{15\,634\,410}$ modulo p pour trouver le résultat 100928. Mais sur le même ordinateur, avec un programme tapé dans le même langage, la résolution de l'équation en n : $53^n = 100928\ [21997783]$ a pris 39 secondes, soit 300000 fois plus!

Il est intéressant de se pencher sur la raison de ce décalage.

Prenons l'exemple du calcul de a^{106}. La première idée est que 105 multiplications sont nécessaires. Mais c'est compter sans le soutien du système binaire: l'écriture 106 = 2+8+32+64 fournit $a^{106} = a^2 \times a^8 \times a^{32} \times a^{64}$. On commence donc par calculer de a^2 à a^{64} par élévations au carré successives (6 multiplications) et puis on multiplie entre elles les puissances concernées (trois multiplications). Ainsi le calcul de a^{106} n'a demandé que 9 multiplications … et non pas 105.

De façon analogue, le calcul de $53^{15634410}$ ne nécessite que 38 multiplications.

Par contre, les restes de 53^n modulo 21 997 783 ne présentent aucune régularité et ne vont pas croissants. Pour résoudre l'équation $53^n = 100\,928\ [21\,997\,783]$, il n'est d'autre possibilité que de faire évoluer n de 1 en 1 jusqu'à tomber sur le résultat.

Avant d'aboutir à la solution $n = 15634410$, il aura fallu… 15634409 multiplications !

On imagine qu'avec un nombre premier de plusieurs centaines de chiffres et une puissance assez élevée, l'inversion de la fonction, bien que possible, demande des milliards d'années de calcul !

2.3. L'administration du remède

L'idée d'utiliser ces fonctions pour échanger publiquement des clés fait partie du trait de génie de Whitfield Diffie et Martin Hellman.

Imaginons qu'Alice et Bernard disposent d'un procédé de chiffrement connu fondé sur le choix d'une clé numérique (comme le DES par exemple). Par téléphone ou par courrier, ils conviennent d'un nombre p premier et d'un nombre a, $1 < a < p$. Comme exemple, prenons les nombres a et p du paragraphe précédent.

Alice choisit un nombre secret $\alpha = 3660$ et Bernard un nombre secret $\beta = 4307$..

Alice calcule $a^{\alpha} = 11375235\ [p]$ et le transmet à Bernard.

Bernard fait de même en envoyant à Alice $\alpha^{\beta} = 2913121\ [p]$.

Bernard calcule élève alors le nombre envoyé par Alice à la puissance β modulo p, et trouve 10928.

Alice fait de même en élevant le nombre envoyé par Bernard à la puissance α modulo p et trouve également 10928 puisque $(a^{\alpha})^{\beta} = (a^{\beta})^{\alpha} = a^{(\alpha \times \beta)}$.

retour au sommaire

Ils utilisent alors ce résultat pour chiffrer leurs messages avec le procédé convenu.
Imaginons qu'un malfaisant Igor espionne les communication. Il connait a, p, a^{α} [p] et a^{β} [p].
Comme nous l'avons vu précédemment, cela ne lui permettra pas de restituer ni α, ni β, ce qui serait indispensable pour connaitre la clé de chiffrement $a^{(\alpha \times \beta)}$ [p].
Sans l'échanger concrètement, Alice et Bernard ont pu convenir d'une clé de chiffrement commune.

2.4. La faille du remède

Dans un procédé d'encryptage donné, l'utilisation répétée d'une même clé présente un danger : celui de fournir à un espion trop de textes chiffrés exactement de la même façon. Pour des questions de sécurité, il est bon de changer les paramètres de chiffrement régulièrement (pendant le dernière guerre, la clé de la machine *Enigma* changeait tous les jours).
Imaginons qu'Alice et Bernard résident dans deux pays à fort décalage horaire et ne puissent facilement être en ligne en même temps. Alice veut envoyer un message crypté à Bernard. Elle lui envoie les nombres qu'elle a choisis : a, p et a^{α}. Bernard consulte sa boite quelques heures plus tard, renvoie à Alice son nombre a^{β} et calcule la clé. Encore plus tard, Alice relève sa boite aux lettres et peut alors, elle aussi, calculer la clé. Elle envoie alors à Bernard le message chiffré que ce dernier lira lorsqu'il se réveillera, encore plus tard.
Whitfield Diffie et Martin Hellman sentaient que cette multiplicité d'échanges avant de pouvoir communiquer créait un handicap. Qui plus est, la fuite et l'intoxication restent possibles avec ce procédé : n'importe qui peut se faire passer pour l'un des deux en piratant sa boite à lettres sans que l'autre ne se doute de quoi que ce soit.
Ils cherchèrent mieux : un moyen pour qu'Alice puisse directement laisser sur la boite à lettres de Bernard un message crypté en étant sûre que lui seul pourrait le déchiffrer. Il fallait donc que la clé de chiffrement de Bernard soit connue de tous …, mais que lui seul possède la clé de déchiffrement. Cela serait comparable à un cadenas que tout le monde peut fermer, mais que seul le détenteur de la clé peut ouvrir. N'importe qui pourrait acheter en magasin un cadenas ouvert de type *Bernard*, enfermer le message dans une boite et l'envoyer à Bernard, sachant que lui seul possède la clé pour ouvrir ce type de cadenas.
La solution fut trouvée en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman qui inventèrent le RSA (initiales de leurs inventeurs), protocole de chiffrement à clé révélée.

3. LE GRAAL : UN CHIFFREMENT À CLÉ RÉVÉLÉE

3.1. Le but de la manœuvre

Outre le fait de conserver la confidentialité d'un message, un procédé de chiffrement doit aussi éviter les intoxications. C'est à dire que l'émetteur doit être sûr que seul le destinataire pourra le déchiffrer, et le récepteur doit être sûr que le message a bien été envoyé par l'expéditeur présumé.

3.2. Les vertus d'une clé révélée

Un tel procédé est fondé sur l'existence de fonctions mathématiques bijectives f qui servent à chiffrer les messages et qui sont connues de tous, mais dont, pour chacune d'entre elles, la réciproque f^{-1} n'est connue que d'une personne (le propriétaire de la fonction), et impossible à déterminer à partir de f.
Pour en comprendre l'intérêt, supposons qu'il existe un tel procédé. Dans un annuaire, nous allons trouver la fonction f_A (resp. f_B) attribuée à Alice (resp. Bernard), dont seule Alice (resp. Bernard) connait la fonction réciproque f_A^{-1} (resp. f_B^{-1}).
Alice veut envoyer le message T (texte clair) à Bernard. Elle se procure dans l'annuaire f_B, calcule $T' = f_B \circ f_A^{-1}(T)$ et fait parvenir T' à Bernard.
Pour déchiffrer ce message, il faudra lui appliquer $f_A \circ f_B^{-1}$.
Alice est donc sûre que seul Bernard pourra le lire puisque lui seul connait f_B^{-1}.
Mais quand Bernard aura appliqué f_B^{-1} au message crypté reçu, il n'obtiendra pas un message clair. Comme le message est sensé provenir d'Alice, Bernard se procurera la clé publique f_A et l'appliquera au résultat

retour au sommaire

obtenu. S'il obtient un message clair *T*, il saura alors que celui-ci provient bien d'Alice puisqu'elle seule pouvait le crypter avec f_A^{-1} .

3.3. Où poussent de telles fonctions ?

Le système repose encore cette fois sur des manipulations facilement réalisables dans un sens et extrêmement longues dans l'autre sens, donc considérées comme impossibles.
En fait Alice va partir de f_A^{-1} pour construire f_A (manipulation aisée) qu'elle communiquera à tout le monde, sachant qu'il faudrait des années pour retrouver f_A^{-1} à partir de f_A.
Évidemment la technologie évolue et un calcul nécessitant un siècle à un moment donné peut très bien se voir réduit à quelques secondes cinq ans plus tard. Mais cela est-il vraiment grave que les documents soient décryptés cinq ans plus tard ? Et les mathématiques permettent souvent d'augmenter la difficulté en choisissant des nombres plus grands pour augmenter les temps de calcul de façon exponentielle, ou en découvrant des nouvelles fonctions pathologiques au comportement exaspérant.
Nous analyserons dans les sections suivantes deux exemples de chiffrement à clef révélée.

3.4. Codage numérique d'un texte

Le chiffrement par fonction mathématique suppose déjà un codage numérique des caractères. Le code ASCII étendu (de 0 à 255) permet de transformer en nombre les caractères alphanumériques d'un texte, ainsi que les ponctuations et les lettres accentuées. Nous utiliserons donc dans la suite le code ASCII, chaque caractère du texte étant alors représenté par un octet.

4. CHIFFREMENT PAR EMPILEMENT

4.1. Un problème difficile

Considérons un ensemble de 16 pièces dont les hauteurs sont données par le vecteur *A*' :
A' = (65455 ; 51479 ; 9551 ; 33078 ; 52180 ; 24929 ; 63834 ; 34261 ; 68522 ; 71589 ; 35795 ; 6135 ; 77725 ; 78122 ; 70285 ; 61139), et j'empile certaines de ces pièces sans vous dire lesquelles en vous livrant la hauteur totale obtenue : 279 095. A votre charge de retrouver les pièces utilisées !
Nous admettrons pour l'instant qu'une seule configuration peut donner l'empilement dont il est question. L'algorithme le plus rapide connu pour résoudre ce problème consiste à envisager chacune des 2^{16} possibilités. Dans notre exemple, cela reste accessible à tout ordinateur … mais imaginez ce que cela peut donner avec un vecteur à 1000 coordonnées : le nombre de cas à envisager dépasse le nombre d'atomes actuellement estimé dans l'univers !

4.2. Un problème facile

Reprenons le même problème que dans le paragraphe précédent, mais cette fois avec le vecteur *A*' = (1 ; 2 ; 5 ; 9 ; 19; 38 ; 75; 151 ; 302 ; 603 ; 1208 ; 2415 ; 4831 ; 9713 ; 19381 ; 38762) et une pile de taille 23765.
Comme vous l'avez tout de suite remarqué au premier coup d'œil, le vecteur *A*' est très particulier : chacune de ses coordonnées est supérieure à la somme des précédentes.
La pièce 16 (38762) n'a visiblement pas été prise et on peut affirmer que la pièce 15 (19381) a été utilisée. En effet, si nous ne la prenons pas, la somme de toutes les autres ne l'excédant pas, il sera impossible d'arriver à la hauteur voulue.
Il nous reste à composer la hauteur 23765 - 19381 = 4834 et par un raisonnement analogue, nous trouvons que la pièce n°12 (2415) figure dans la pile.
En continuant ainsi, on trouve le vecteur *X* indiquant les pièces prises :

X = (0 ; 1 ; 1 ; 0 ; 0 ; 0 ; 0 ; 1 ; 0 ; 1 ; 1 ; 1 ; 0 ; 0 ; 1 ; 0)

On vérifie aisément que le produit scalaire *A'*. *X* vaut bien 23765.

retour au sommaire

4.3. Comment transformer un problème difficile en un problème facile ?

Vous l'avez compris : le vecteur *A* n'est pas tout à fait, et même pas du tout, aléatoire. Ce n'est qu'un brouillage du vecteur *A'* : il est issu du vecteur *A'* via une bijection difficilement inversible.

Considérons les entiers $m = 79431$ et $w = 65455$. Ces deux nombres sont premiers entre eux. Donc *w* est inversible dans $\mathbf{Z}/m\mathbf{Z}$ et son inverse w^{-1} est obtenu via l'algorithme d'Euclide et l'identité de Bezout.

Ainsi, l'application $\Phi : \; a \in \mathbb{Z}/m\mathbb{Z} \to a \times w\,[m]$ est une bijection. Je vous laisse le soin de vérifier que $\Phi(A') = A$.

De plus, *m* étant supérieur à la somme des coordonnées de *A'*, le travail dans $\mathbf{Z}/m\mathbf{Z}$ permet de discriminer simplement toutes les piles qu'on peut obtenir avec *A'*.

Une personne connaissant *A* ne peut pas retrouver le vecteur *A'* s'il ne connait pas les nombres *m* et *w*.

Nous verrons dans la suite que *A* est la clef révélée de ce procédé et que *m* et *w* en constituent la clef secrète, encore appelée la gâche du chiffrement par empilement.

4.4. Mathématisons un peu

Pour $n \in \mathbb{N}^*$ soit $\mathcal{E} = \{0\,;\,1\}^n$ l'ensemble des vecteurs *x* à coordonnées binaires et posons :

$$\mathcal{A}' = (a'_1\,;a'_2\,;\cdots;a'_n) \in (\mathbb{N}^*)^n, \forall k \in \{2\,;3\,;\cdots;n\}, a_k > \sum_{i=1}^{i=k-1} a_i$$

$$\text{Soit } m \in \mathbb{N}, m > \sum_{i=1}^{i=n} a_1 \;,$$

soit $w \in \{2\,;3\,;\cdots;m-1\}, w \wedge m = 1, \alpha \in \mathbb{Z}/m\mathbb{Z} \xrightarrow{\phi} \alpha \times w\,[m], w' = w^{-1}\,[m]$,

posons $\mathcal{A} = \phi(\mathcal{A}') = (a_1\,;a_2\,;\cdots;a_n), \forall i \in \{1\,;2\,;\cdots;n\}, a_i = \phi(a'_i)$.

Propriété 4.4.i :

L'application $X \in \mathcal{E} \xrightarrow{\Psi} \mathcal{A}' \cdot X = \sum_{i=1}^{i=n} a'_i \times x_i \in \mathbb{N}$ est injective.

Démonstration : Soient $X, Y \in \mathcal{E}, X \neq Y, \Psi(X) = \Psi(Y)$

$k = max(i \in 1\,;2\,;\ldots n), x_i \neq y_i$ et posons $k = max\, i \in (1\,;2\,;\ldots;n), x_i \neq y_i$

On a donc $\forall i \in \{k+1\,;\cdots;n\}, x_i = y_i$ et $x_k \neq y_k$.

Supposons $x_k = 1, y_k = 0$.

Soit $Z = (0\,;0\,;\cdots;0\,;x_{k+1}\,;\cdots;x_n) = (0\,;0\,;\cdots;0\,;y_{k+1}\,;\cdots;y_n)$

Par propriété du produit scalaire, on a $\Psi(X - Z) = \Psi(Y - Z)$

Si k = 1, cela signifie $a' = 0$, ce qui est faux, et si k>1, cela conduit à

$$a'_k \leq \sum_{i=1}^{i=k-1} x_i \times a'_i + 1 \times a'_k = \sum_{i=1}^{i=k-1} y_i \times a'_i + 0 \times a'_k < \sum_{i=1}^{i=k-1} a'_i$$

ce qui est contradictoire avec la construction du vecteur A'.

Donc l'application Ψ est bien injective.

retour au sommaire

Propriété 4.4.ii :

L'application $\mathcal{X} \in \mathscr{E} \xrightarrow{\Psi} \mathcal{A}\ '\cdot\mathcal{X}\ [m] \in \mathbb{Z}/m\mathbb{Z}$ est injective.

Démonstration : L'image de Ψ étant contenue dans [0 ; *m*-1] par choix de l'entier $m > \sum_{i=1}^{i=n} a_i$, cette propriété est une conséquence de la précédente.

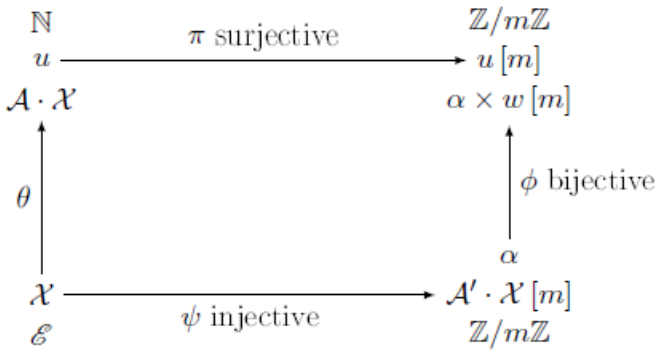
Propriété 4.4.iii :

L'application $\alpha \in \mathbb{Z}/m\mathbb{Z} \xrightarrow{\phi} \alpha \times w\,[m] \in \mathbb{Z}/m\mathbb{Z}$ est bijective.

Cela est simplement dû au fait que w est inversible dans $\mathbb{Z}/m\mathbb{Z}$.

Propriété 4.4.iv :

Dans le schéma suivant :



Cela provient directement de la définition de *A* à partir de *A'* :

$$\phi\circ\psi(\mathcal{X}) = \left(\sum_{i=1}^{i=n} a'_i \times x_i\right) \times w[m] = \left(\sum_{i=1}^{i=n} a'_i \times w \times x_i\right)[m] = \left(\sum_{i=1}^{i=n} a_i \times x_i\right)[m] = \pi\circ\theta(\mathcal{X})$$

Propriété 4.4.v :

L'application $\mathcal{X} \in \mathscr{E} \xrightarrow{\theta} \mathcal{A}\cdot\mathcal{X} \in \mathbb{N}$ est injective.

Démonstration : $\Phi_o\Psi$, composée d'une bijection et d'une injection, est injective.
Avec [4.4.*iv*], on en déduit que $\pi_o\theta$ est injective, et donc cela entraine que θ est injective.

Conséquences : Cela établit qu'un entier obtenu comme somme d'éléments de *A* ne peut l'être que d'une seule façon.

Cela nous fournit aussi un moyen de retrouver $\mathcal{X}$ à partir de $N = \mathcal{A}\cdot\mathcal{X} = \theta(\mathcal{X})$ lorsqu'on connait *m* et *w* :

- considérer $N' = w^{-1} \times N[m] = \phi^{-1}\circ\pi(N)$
- nous avons donc $N' = \phi^{-1}\circ\pi\circ\theta(\mathcal{X}) = \psi(\mathcal{X})$
- or, nous avons vu au §[4.2] comment retrouver $\mathcal{X}$ à partir de $\psi(\mathcal{X}) = \mathcal{A}\ '\cdot\mathcal{X}$

Reprenons l'exemple du §[4.1] avec *N* = 279095.

Nous avions vu au §[4.3] que $\mathcal{A}$ était obtenu à partir de $\mathcal{A}'$ avec *m* = 79431 et *w* = 65455.
Nous avions également mentionné que w^{-1} = 1813 dans $\mathbb{Z}/m\mathbb{Z}$.
Prenons $N' = w^{-1} \times N[m]$ = 1813x279095 [79431] = 23765 .

Le §[4.2] détaille la décomposition de 23765 suivant les coordonnées de $\mathcal{A}'$.

Et nous obtenons ainsi le vecteur $\mathcal{X} = (0;1;1;0;0;0;0;1;0;1;1;1;0;0;1;0)$ tel que $\mathcal{A}\cdot\mathcal{X} = 279095$.

retour au sommaire

4.5. Et le chiffrement dans tout ça ?

Le texte à chiffrer est scindé en groupes de deux caractères (espaces et ponctuations sont des caractères). Chaque caractère pouvant être représenté par un octet (voir table ASCII), chaque groupe de deux caractères correspond, en les accolant, à un vecteur *x* de 16 coordonnées binaires.
Par exemple, le groupe **ar** correspond au vecteur *X* =(0 ; 1 ; 1 ; 0 ; 0 ; 0 ; 0; 1 ; 0 ; 1 ; 1 ; 1 ; 0 ; 0 ; 0) du §[4.2] puisque le code ASCII du **a** est 97 = $[01100001]_2$ et celui du **r** vaut 114 = $[01110010]_2$.

Imaginons que Alice ait choisi en secret les nombres *m* et *w* déjà évoqués, ainsi que le vecteur *A'*. Elle a alors calculé *A* = *w*x*A'* [*m*] et l'a publié dans un annuaire (clé révélée).
Bernard veut envoyer un texte clair à Alice et trouve dans l'annuaire sa clé révélée *A*.Il chiffre **ar** par le produit scalaire *A*x*X* = 279095.
Pour déchiffrer la signification de ce nombre dans le message reçu, Alice utilisera sa clé secrète (*m* ; w^{-1} ; *A'*) qu'elle est la seule à connaitre, selon le protocole expliqué dans l'exemple ci-dessus.

Si vous voulez tester un algorithme de chiffrement par cette méthode, vous pourrez vérifier que le texte **J'arriverai le 12 à 7 h** donne la séquence chiffrée `412834 – 279095 – 404190 – 429516 – 326465 – 183266 – 384784 – 112620 – 142258 – 162280 – 201448 – 375137 ;` et que le message chiffré `414138 – 201192 – 301098 – 310678 – 453736 – 330902` signifie : **Je t'attends**

5. LE CHIFFRE RSA

5.1. Un problème difficile

Décomposer un nombre dont on sait que c'est le produit de deux premiers.
Essayez pour voir avec 29 083. Il faut déjà obtenir tous les premiers à concurrence de sa racine (crible d'Eratosthène). Ici donc de 2 à 170.
Supposons qu'on en ait la liste. Il vous faudra bien une bonne heure à la main pour tester les divisibilités et aboutir au 31e nombre premier qui est 127 et trouver que 29083 = 127x229.

Sur de grands nombres (quelques centaines de chiffres), le temps de calcul informatique croît de façon exponentielle et peut atteindre des dizaines de siècles.

5.2. Un problème facile

Calculer le produit de deux nombres premiers.
À la main, la multiplication de 127 et 229 prend une paire de minutes.
Pour des nombres premiers comportant un grand nombre de chiffres (quelques centaines), un ordinateur effectue le calcul en quelques secondes.

5.3. Un résultat arithmétique utile

Propriété 5.3.i :

Soient *p* et *q* deux nombres premiers, et posons *n* = *p*x*q* et *m* = (*p*-1)x(*q*-1) .

Soit $e \in 2\,;3\,;\ldots;m-1\,,e\wedge m=1$ et *d* l'inverse de *e* modulo *m*.

Soient a et b dans {1; 2 ;...; n-1}. Alors on a : $b \equiv a^e[n] \Leftrightarrow a \equiv b^d[n]$

Démonstration :
Le fait qu'on a aussi $e = d^{-1}[m]$ et que *d* est aussi premier avec *m* rend cette équivalence symétrique et il suffit donc de démontrer une seule implication.

$$b \equiv a^e[n] \Rightarrow b^d \equiv a^{ed}[n]$$

$$e \times d \equiv 1[m] \Rightarrow \exists k \in \mathbb{N}, e \times d = k \times m + 1$$

$$b \equiv a^e[n] \Rightarrow b^d \equiv a^{km} \times a[n]$$

retour au sommaire

Si a $a \wedge n = 1$, alors *a* appartient au groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$; comme $n = p \times q$ avec *p* et *q* premiers, ce groupe contient (*p*-1)(*q*-1) éléments (voir fonction d'Euler) ; *a* étant dans un groupe multiplicatif d'ordre *m*, on $a^m \equiv 1[n]$, et donc $a^{km} \equiv 1[n]$ et finalement on obtient : $a^{km} \times a \equiv a[n]$

- Si $a \wedge n \neq 1$, comme $n = p \times q$ avec *p* et *q* premiers, cela signifie que *a* est un multiple de *p* ou de *q,* et $a < n$ implique que *a* ne peut être multiple à la fois de *p* et *q.*
  Disons par exemple que *a* est multiple de *p* mais pas de *q* ; alors *a* est premier avec *q,* et dans le groupe multiplicatif dans le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$, on a $aq^{-1} \equiv 1[q]$
  et donc $a^m = a^{(p-1)(q-1)} \equiv 1[q]$ et a fortiori $a^{km} \equiv 1[q]$, ce qui signifie que $a^{km} - 1$ est un multiple de *q* ; et comme *a* est un multiple de *p*, cela induit que $(a^{km} - 1) \times a$ est un multiple de *pq*, c'est à dire *n*.
  Finalement cela donne : $a^{km} \times a - a \equiv 0[n]$ et donc, là encore, $a^{km} \times a \equiv a[n]$

  L'implication $b \equiv a^e[n] \rightarrow b^d \equiv a[n]$ est ainsi démontrée, et par symétrie la propriété aussi.

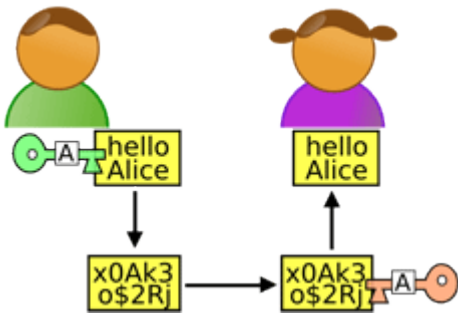
5.4. Chiffrer en RSA

Alice prend par exemple *p* = 479 et *q* = 541 et obtient *n* = 259139 et *m* = 258120.
Elle choisit *e* = 359, premier avec *m*, et calcule son inverse modulo *m* : *d* = 719.
Elle publie dans un annuaire sa clé publique (*n* ; *e*).
Bernard veut crypter **ar** dans un message destiné à Alice. Il accole les deux nombres décimaux (formatés sur 3 chiffres) représentant ces deux caractères en code ASCII et obtient a = 097114..
Remarquons qu'il obtiendra toujours un nombre inférieur à 255255, donc inférieur à *n*.
Il calcule a^e modulo *n* et obtient *b* = 156229, et ce nombre cryptera **ar** dans le message.

Avec la clé publique d'Alice, le message **J'arriverai le 12 à 7 h** va ainsi être chiffré
`195483 – 156229 – 133380 – 228039 – 31701 – 39311 – 87362 – 123219 – 67354 – 159742 – 154974 – 7403.`

5.5. Déchiffrer du RSA

Alice veut déchiffrer la séquence cryptée par *b* = 111116
En vertu de la propriété [5.3.i], elle va calculer b^d modulo *n,* va trouver *a* = 74101et identifier le caractère **J** par son code ASCII 74 et **e** par son code ASCII 101.
Par exemple, le message crypté `111116 – 140003 – 181943 – 4277 – 58734 – 32095` sera déchiffré par Alice en : **Je t'attends**
Nous voyons là que pour déchiffrer, la connaissance de *d* est indispensable. Or *d* ne peut être déterminé qu'en connaissant *m*, et donc en connaissant *p* et *q*. Pour retrouver *p* et *q* à partir de leur produit, le temps de calcul serait astronomique si les nombres premiers choisis par Alice comportaient plusieurs centaines de chiffres.



retour au sommaire

DU « CARRÉ DE POLYBE » AU « RADIOGRAMME DE LA VICTOIRE » DE JUIN 1918

par François DROUIN

Dans un carré 5×5, je place les vingt-six lettres de notre alphabet latin. Il n'y a que vingt-cinq cases, I et J sont regroupés.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I /J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

A chaque lettre correspond un couple formé d'un nombre rouge et d'un nombre noir. « APMEP » va être codé 11 53 23 51 53 et pourrait être transmis sous sa forme chiffrée ou en utilisant des signaux différents pour les nombres rouges et les nombres noirs (le « P » pourrait correspondre à cinq signaux d'une couleur suivis de trois signaux d'une autre couleur).
Cette méthode de codage est celle du « carré de Polybe » : Polybe a vécu en Grèce vers -200, mais son carré était encore utilisé par les nihilistes russes vers 1900 : ils communiquaient entre eux dans leurs prisons à l'aide de coups brefs et de coups longs sur les tuyaux de leurs cellules, il n'est donc pas surprenant que plus tard l'alphabet morse ait été utilisé par la suite pour ce codage.
Nous retrouvons l'utilisation d'un « carré de Polybe » à la page 53 du récit des aventures de Blake et Mortimer, « Le bâton de Plutarque » paru fin 2014. Les nombres en tête de ligne et de colonne indiquent des flashs vus à droite et des flashs vus à gauche. Il n'est cependant pas précisé comment le Professeur Mortimer a compris que ces éclairs lumineux avaient pour source un codage à l'aide d'un tel carré.

Cette méthode de codage a ensuite été améliorée pour pouvoir coder des chiffres. Vingt-six lettres et dix chiffres amènent à l'utilisation d'un carré 6×6. Par ailleurs, pour le codage des lignes et des colonnes les lettres A, D, F, G, V, X ont été utilisées pour leurs codes en morse très différents les uns des autres, permettant d'éviter les erreurs de transmission radio.

A	D	F	G	V	X
· –	– · ·	· · – ·	– – ·	· · · –	– – · · –

retour au sommaire

Les vingt-six lettres et les dix chiffres sont disposés selon notre envie dans le carré 6×6.

	A	D	F	G	V	X
A	A	6	E	O	D	Y
D	H	U	3	L	X	I
F	Z	9	B	5	M	4
G	N	J	Q	F	7	T
V	C	P	2	G	K	1
X	V	R	8	W	S	0

« L'APMEP LORRAINE EN 2018 » se code « GD AA DV VF FA DV FA AG FV XX XV FX ». Je choisis le mot « CUBE » qui va me servir de clé de codage. J'écris le message obtenu dans un rectangle 4×6. Je repère chaque colonne par une des lettres de mon mot clé.

C	U	B	E
G	D	A	A
D	V	V	F
F	A	D	V
F	A	A	G
F	V	X	X
X	V	F	X

B	C	E	U
A	G	A	D
V	D	F	V
D	F	V	A
A	F	G	A
X	F	X	V
F	X	X	V

J'ai réordonné les colonnes du tableau selon l'ordre alphabétique des lettres de mon mot clé. « AGADVDFVDFVAAFGAXFXVFXXV » est le message que je transmettrai.
Sans connaître mon mot clé et mon tableau de départ, le déchiffrage sera ardu…

Et pourtant…

Le 1er juin 1918, les services du chiffre de l'armée française recevaient le message FGAXA XAXFF FAFVA AVDFA GAXFX FAFAG DXGGX AGXFD XGAGX GAXGX AGXVF VXXAG XDDAX GGAAF DGGAF FXGGX XDFAX GXAXV AGXGG DFAGG GXVAX VFXGV FFGGA XDGAX FDVGG A

Le lieutenant Georges-Jean Painvin réussit à retrouver la clé (un ensemble de 21 lettres…) ainsi que la grille de départ et décode le message.

Munitionierung beschleunigen Punkt soweit nicht eingesehen auch bei Tag (« hâter l'approvisionnement en munitions, le faire même de jour tant qu'on n'est pas vus »).

L'attaque se produisit le 10 juin 1918, mais l'État Major français prévenu a pu prendre ses dispositions. Au vu de l'importance qu'a eu ce message, il est actuellement appelé « Radiogramme de la Victoire ».

retour au sommaire

Le système utilisé par l'armée allemande et repris en début de cet article était nommé GEDEFU 18 (*GEheimschrift DEr FUnker 18*, « chiffre des radiotélégraphistes 18 ») et avait été conçu en 1918 par le colonel Fritz Nebel. Il fallut attendre les années soixante pour que soit connu ce qu'avait fait le lieutenant Georges-Jean Painvin, Fritz Nebel lui-même ne l'apprit que quelques années plus tard… Les secrets militaires sont bien gardés.

Éléments de sitograhie

http://www.bibmath.net/crypto/index.php?action=affiche&quoi=substi/polybe Pour en savoir plus à propos des « carrés de Polybe ». Le site fournit de quoi coder et décoder vos messages.

http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/radiogramme Pour en savoir plus sur le radiogramme de la Victoire.

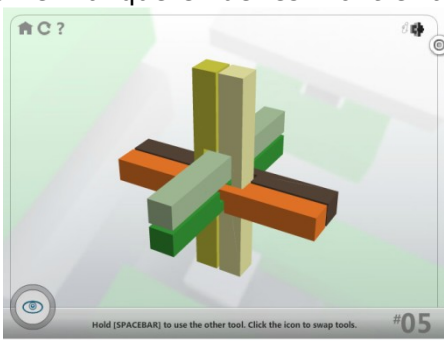
http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/adfgvx Pour en savoir plus à propos du code « ADFGVX ». Le site fournit de quoi coder et décoder vos messages.

http://www.annales.org/archives/x/painvin.html Pour en savoir plus à propos de Georges-Jean Painvin.

retour au sommaire

ENTRAÎNEZ-VOUS !

Pour ceux qui auraient laissé passer l'info, je me permets de rappeler que la prochaine semaine des maths aura pour thème le jeu (et les maths bien sûr !). Quelque chose me dit que l'on ne va pas se limiter à une semaine. Cela fait déjà quelques temps que je voulais vous proposer quelques références de jeux en ligne du type « jeux flash », qui peuvent être qualifiés, pour la plupart d'entre eux, de jeux chronophages. Nos vacances d'été sont souvent ponctuées de jours de pluie que vous mettrez à profit pour vous mesurer à quelques un de ces défis vidéo-ludiques et prendre de l'avance sur vos élèves, auxquels vous ne manquerez de les montrer à la rentrée.

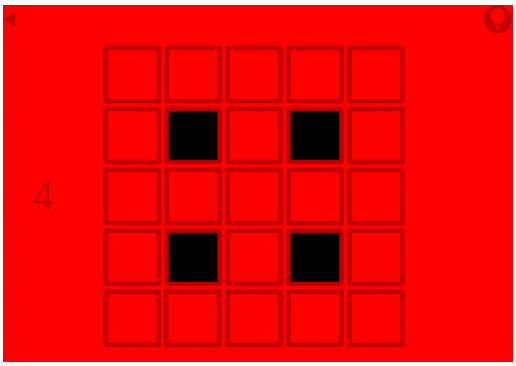


Deux sites s'imposent, à mon sens, comme référence dans ce domaine : ArmorGames et Kongregate. La qualité des jeux présentés est très variable, mais on y trouve régulièrement des jeux de réflexion d'un bon niveau.

En lien avec la mécanique, on pourra ainsi tester Interlocked, où il faut désassembler des pièces comme dans ces casse-têtes en bois, ou chercher à maintenir l'équilibre d'empilements savants dans Super Stacker 2 .

Les jeux dits « de chemins » sont également très nombreux sur le Web. J'y classerai Hexallin où il faut construire un réseau sur des tuiles hexagonales. Dans un autre genre, on essaiera de créer, en quelques étapes, le plus grand ensemble connexe dans ColorUID 2 (il ne faut pas s'arrêter à son apparence). Enfin, Apple Worm a un côté déjà-vu et, pourtant, ses graphismes enfantins ne sauraient dissimuler des situations complexes.

Comme le cinéma, le jeu vidéo se scinde entre grosses productions et auteurs indépendants. Ces derniers proposent des créations personnelles dans lesquelles le manque de moyens est compensé par une grande inventivité dans les formes de jeu et par des choix graphiques qui dénotent une sensibilité artistique indéniable. Hoshi Saga propose ainsi une série de jeux d'énigme dont l'unique but est de faire apparaître une étoile à cinq branches, par tous les moyens possibles et imaginables. Toujours du côté du soleil levant, EyezMaze a créé plusieurs scénettes (intitulées « grow ») dans lesquelles il faut enchaîner des actions dans un certain ordre. Par exemple, dans Grow Cube, on devra effectuer plusieurs essais pour découvrir les chaînes de conséquences et assurer le meilleur résultat final.



On terminera par un auteur belge que j'apprécie tout particulièrement, Bart Bonte, qui réalise des jeux aussi esthétiques qu'innovants. Le dernier en date, Red, succède assez logiquement à Yellow. Tout au long de ces petites énigmes visuelles, il faut en général commencer par chercher la règle du jeu (souvent simple) avant de résoudre le problème (une ampoule d'aide vous assistera en cas de besoin). Je ne peux m'empêcher de vous soumettre également Factory Balls qui requiert une bonne analyse des motifs pour retrouver la suite des coloriages à exécuter.

stephanie.waehren@wanadoo.fr et gilles.waehren@wanadoo.fr

retour au sommaire

PLAISIR ET BONHEUR

Par Didier Lambois

Si nos élèves ne réussissent pas dans notre matière c'est qu'ils ne s'y impliquent pas suffisamment, et s'ils ne s'impliquent pas c'est parce qu'ils n'y trouvent pas suffisamment de plaisir. C'est donc par le plaisir que nous pourrions faire naître l'intérêt et par conséquent la réussite des élèves. Voilà grossièrement le raisonnement que font les professeurs soucieux de bien faire, et c'est ce type de raisonnement qui conduit aussi les plus éminents mathématiciens à dire qu'il faut « *rendre les maths sexy* ». Sans vouloir juger de la pertinence de tels propos, prenons le temps d'y réfléchir quelques minutes.

Il faut tout d'abord s'entendre sur ce que nous appelons le plaisir. Nous dirons que nous éprouvons du plaisir lorsque nous rencontrons quelque chose qui satisfait l'une de nos tendances, l'un de nos désirs. J'ai soif et je bois, alors j'éprouve du plaisir ; je désire résoudre un problème mathématique et j'y parviens, alors j'éprouve du plaisir. C'est donc le désir qui est en jeu ici, et ce n'est pas trahir la formule citée ci-dessus que de dire « *il faut rendre les maths désirables* ».

Cela sous-entend que ce sont les objets qui déterminent nos désirs. Si un objet est désirable, nous le désirons… En conséquence nous devrions admettre que nous désirons tous les mêmes objets : ceux qui sont désirables. Est-ce aussi simple ? Ce qui est désirable pour moi l'est-il nécessairement pour autrui ? Est-ce vraiment l'objet qui détermine notre désir ou est-ce au contraire notre désir qui fait la valeur de l'objet ? Spinoza affirmait que « *nous ne nous efforçons à rien, ne voulons, n'appétons ni ne désirons aucune chose parce que nous la jugeons bonne ; mais, au contraire, nous jugeons qu'une chose est bonne parce que nous nous efforçons vers elle, la voulons, appétons et désirons* » (Spinoza, *Ethique, III).*

Certains jugent que les mathématiques sont « bonnes » et pour eux elles sont « sexy », elles donnent du plaisir, un plaisir plus fort même et plus durable que le plaisir sexuel disait André Weil. Ceux qui ont la fibre mathématique et qui ont ce désir mathématique, connaissent ce plaisir, c'est indéniable, mais pouvons-nous créer ce désir chez tous nos élèves ? Là est le problème et là nait le doute.

Peut-être faudrait-il penser les mathématiques (et la vie en général) dans la perspective du bonheur plutôt que dans celle du plaisir. Mais il faut alors s'entendre sur ce que serait le bonheur et sur ce qui le distingue du plaisir.

La définition du bonheur est problématique, chacun semble en avoir une idée différente, et une idée souvent confuse. Même si nous cherchons tous le bonheur nous ne savons pas bien ce que nous cherchons. « *Nous cherchons tous le bonheur, mais sans savoir où, comme des ivrognes qui cherchent leur maison, sachant confusément qu'ils en ont une* » disait Voltaire. Pour y voir plus clair nous nous contenterons de dire que le bonheur n'existe que si nous sommes pleinement satisfaits de ce qui est, pleinement satisfaits de ce que nous faisons et de ce que nous sommes.

Ce qui est ne dépend pas toujours de nous et nous devons le comprendre, l'accepter et même le vouloir, c'est là toute la sagesse stoïcienne et c'est une sagesse qu'il est bien difficile d'atteindre. Mais ce que nous faisons, ce que nous pensons, ce que nous sommes, dépend de nous[2]. Nous serons heureux si nous avons le sentiment de bien faire ce que nous **devons** faire, et d'être pleinement ce que nous **devons** être. Et il faut insister ici sur l'idée de **devoir**. Ce que nous devons être n'est pas nécessairement ce que nous désirons être. Nous savons que le désir nous mène parfois à faire des choses mauvaises pour nous, et désir d'être ceci ou cela

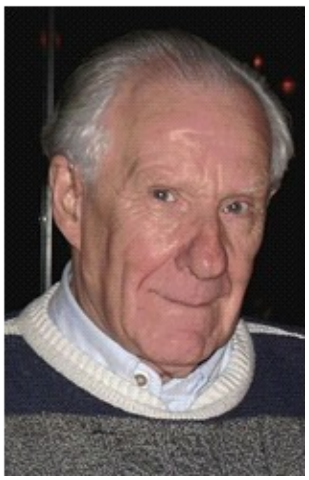
[2] Bien sûr nous ne choisissons pas ce que nous sommes, nous ne choisissons pas notre corps, nous ne choisissons pas notre famille, notre état de santé etc. En ce sens « nous sommes faits », mais nous sommes condamnés à choisir ce que nous allons être à partir de ce qu'on a fait de nous, condamnés à prendre la responsabilité de ce que nous sommes. C'est ce que nous enseigne l'existentialisme de Sartre.

retour au sommaire

ne conduit souvent qu'à un désir de paraître qui ne peut donner aucune satisfaction authentique : on ne peut pas tricher avec le bonheur.

« Il n'est rien si beau et légitime que de faire bien l'homme et dûment, ni science si ardue que de bien et naturellement savoir vivre cette vie » dit Montaigne. « *Faire bien l'homme* », se faire homme, réaliser son humanité comme elle se doit d'être, « *dûment* », c'est la condition d'une pleine satisfaction de soi, la condition du bonheur. Nous sommes en accord avec nous-mêmes lorsque nous avons le sentiment d'avoir fait notre devoir d'homme. En ce cas c'est donc la vertu[3], et non la satisfaction des désirs, qui conduit au bonheur.

Se faire plaisir et faire son devoir d'homme sont deux choses bien différentes, même si l'un n'exclut pas l'autre et réciproquement. Mais lorsque nous ne savons pas trouver de plaisir à ce que nous faisons, peut-être devons-nous nous efforcer de comprendre que c'est notre devoir d'homme, et alors nous y trouverons une satisfaction. Pour celui qui n'a pas la fibre mathématique et qui peut-être ne l'aura jamais, quand bien même nous lui promettrions du plaisir, nous devons lui montrer en quoi le devoir mathématique qu'il a à faire participe à son humanisation, à la réalisation de son humanité. Pour ce faire il faut redonner aux mathématiques leur véritable place dans l'éducation ; il faut cesser de regarder les mathématiques comme une simple science de la quantité, comme une simple série de formules ou de théorèmes qui ne servent à rien dans la vie pratique[4] ; il faut, comme le faisait déjà Platon, montrer que par leur rigueur, leur exigence logique, les mathématiques sont essentielles pour nous élever à notre humanité, pour ne plus être uniquement des bêtes qui courent après le « sexy ».



« *Loin d'être l'exercice ingrat ou vain que l'on imagine, les mathématiques pourraient bien être le chemin le plus court pour la vraie vie, laquelle, quand elle existe, se signale par un incomparable bonheur.* » Alain Badiou, *Éloge des mathématiques*, Flammarion.

[3] **VERTU.** Du latin *vir,* homme par opposition à femme *(homo* désignait l'homme en tant qu'espèce). L'adjectif *virilis* signifiait « qui appartient en propre à l'homme », et a donné « viril ». *Virtus* est dérivé de *vir,* et désignait l'ensemble des qualités morales et physiques qui font la valeur d'un homme viril. Ce pouvait être le courage, l'honnêteté, la force physique ou la puissance intellectuelle. Puis le mot désigna toute espèce de qualité ou de mérite, principalement dans le domaine moral, et il s'utilisa pour les femmes (à tel point qu'au moyen âge il était essentiellement synonyme de chasteté). Le sens moral du mot, à savoir la disposition permanente à vouloir le Bien, s'est développé sous l'influence des idées chrétiennes.

[4] Lorsqu'un philosophe condamne les mathématiques avec ce seul argument qu'elles ne servent pas dans la vie de tous les jours (ce qui en plus est faux), il faut espérer qu'il dit cela uniquement par provocation, ou bien alors il n'a rien compris à ce que sont les mathématiques. Conseillons-lui de lire Alain Badiou.

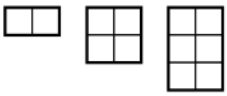
retour au sommaire

MATHS & ARTS

DEVANT UNE BOULANGERIE MOSELLANE (1ère partie)

par François Drouin

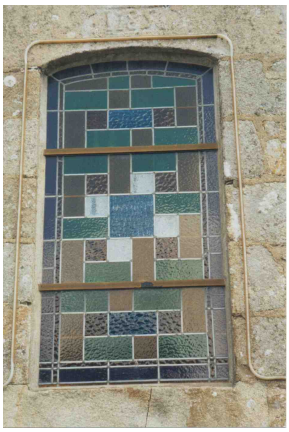
Un de nos adhérents intéressé par le sol devant sa boulangerie favorite, nous a confié cette photographie qui lui semblait être une riche source d'activités mathématiques



Trois types de dalles sont utilisées, correspondant à des rectangles 1×2, 2×2 et 3×2.

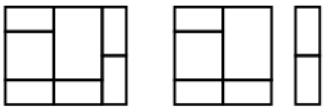
La photographie montre que l'assemblage des pavés n'est traversé entièrement ni par une horizontale, ni par une verticale : cela améliore la solidité du pavement.
Cette caractéristique se retrouve dans bien d'autres situations.

Une porte à la verrerie de Passavant-la-Rochère (70)



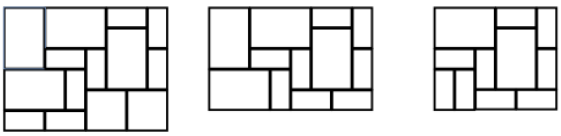
Un vitrail de l'église de Lanmonez (22)

Devant un bâtiment de l'université de Metz, sur l'ile du Saulcy



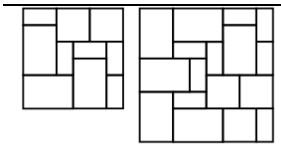
Ces trois rectangles montrent des lignes de brisure verticales ou horizontales.

L'envie vient de rechercher des rectangles ne possédant pas ces brisures et ne pouvant donc pas être décomposés en plusieurs rectangles.



Ces rectangles non carrés ne sont pas décomposables.
En existe-t-il utilisant moins de pièces ?

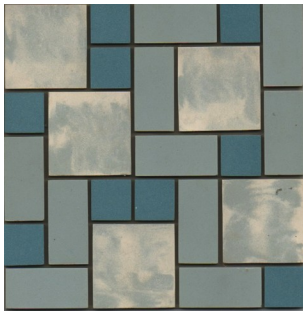
retour au sommaire



Ces carrés ne sont pas décomposables. En existe-t-il utilisant moins de pièces ?

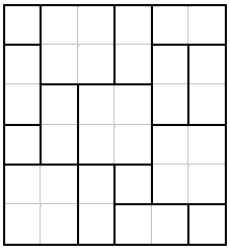
Tout rectangle (carré) est-il recouvrable de cette manière ?

Le carrelage « COMBI »



Le carré commercialisé est un carré « non décomposable ».

Les trois types de pièces sont visualisés par des rectangles 1×2, 2×2 et 3×2. Cinq grands carrés, dix rectangles et neuf petits carrés. Avec ces mêmes pièces, existe-t-il d'autres remplissages non décomposables du carré 7×7 ? En utilisant le même type de pièces, existe-t-ils des carrés « plus petits » recouvrables de la même manière ? Existe-t-il des rectangles recouverts avec moins de pièces ?



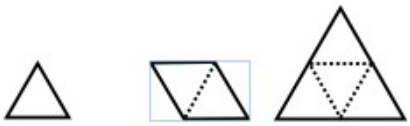
Les pièces proposées pour le « Mini Combi » fournissent un carré plus petit.

Elles sont présentes dans l'exposition « Objets mathématiques » de l'APMEP Lorraine.

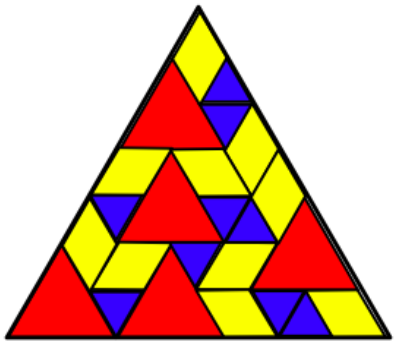
La pose du carrelage « COMBI » laisse cependant apparaître des lignes de fracture entre les lignes et les colonnes formées par les carreaux. Ceux-ci doivent être posés sur un sol bien stabilisé !

retour au sommaire

Un Combi Triangulaire ?



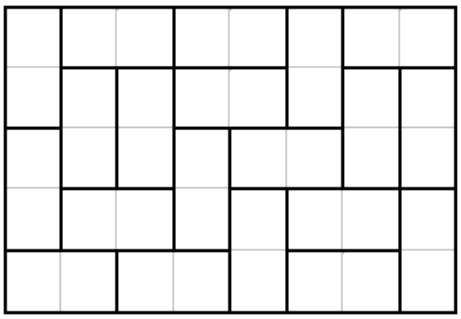
Gardons la même distribution des pièces que pour le Combi carré : quatre grands triangles, huit losanges et neuf petits triangles pour recouvrir un triangle équilatéral de côté 9, dessiné dans un réseau triangulé pour quarante-neuf petits triangles équilatéraux à l'intérieur.



Le triangle rouge en bas à gauche rend cet assemblage décomposable. Existe-il des dispositions des mêmes pièces permettant la création d'un triangle non décomposable ? Et pour des triangles plus petits ?

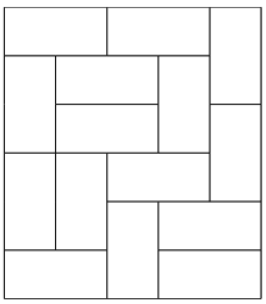
Dans le Petit Vert

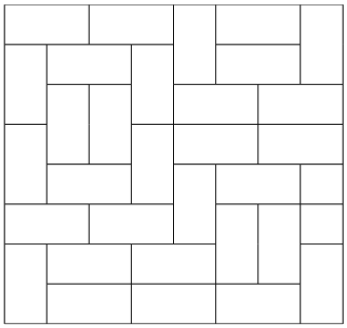
Claude Pagano (La Seyne sur Mer) avait proposé le problème suivant dans le Petit Vert n°58



Ce rectangle de 5x8 est dallé par des dominos (rectangles 2x1) ; il n'admet pas de ligne de fracture, c'est à dire qu'aucune droite ne peut le partager en deux rectangles dallés de dominos. Quel est le plus petit rectangle possédant cette propriété (plus petit signifiant ici d'aire minimum) ? Y a-t-il des carrés possédant cette propriété ?

Voici quelques éléments de solution.





Ces propositions et la preuve qu'on ne peut pas faire mieux sont accessibles sur l'ancien site de la régionale.

Avec des élèves

Dans ce document, un certain nombre de questions sont posées (peu de réponses sont fournies). En classe ou hors la classe, elles pourront devenir des sujets de recherche. Le Petit Vert est preneur d'éléments de réponse.

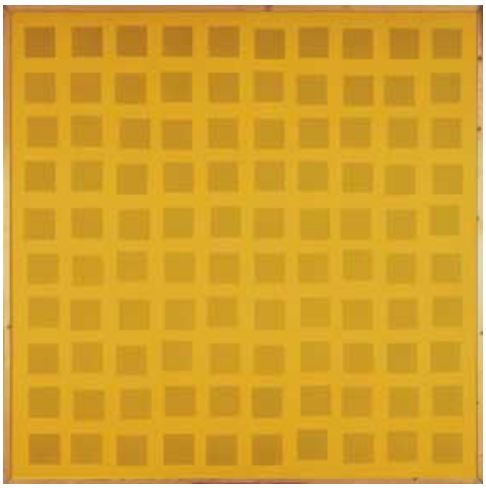
De plus, nos lecteurs trouveront peut-être un peu de temps pour nous confier ce qu'ils ont trouvé.

retour au sommaire

MATHS & ARTS

Fathi Drissi

100 CARRÉS JAUNES
VERA MOLNAR 1977



100 carrés jaunes (*Computer icône 3*). 1977

Acrylique sur toile 152 cm × 152 cm

Collection Frac Basse-Normandie

« Les éléments de base de mon travail sont des formes géométriques simples : des carrés, des rectangles et leurs transformés. Toute mon activité picturale repose sur l'idée que la juxtaposition de formes colorées sur une surface permet parfois d'obtenir un arrangement particulier qui est autre chose qu'une juxtaposition banale de formes banales.
Cette situation visuelle privilégiée qui rend émouvante une portion de surface est nommée « art.
L'emploi de formes élémentaires permet de contrôler pas à pas la genèse de l'image et de localiser l'instant où « le fait d'art » émerge. Pour traquer cet inconnu avec une démarche claire, je me sers souvent d'un ordinateur. La base conceptuelle de la toile Computer – Icône/3 – 100 carrés est une matrice de 10 × 10 carrés. Pour introduire dans ce tissu visuel, parfaitement redondant, un souffle d'air, une respiration, un certain désordre, j'ai déplacé les cent carrés au hasard par le haut, le bas, la gauche, la droite, en x et en y. La forme des carrés est restée inchangée, ce sont les interstices qui se trouvent perturbés. Pour décider de l'importance du désordre, j'ai fait une grande série de dessins-tests sur table traçante, un petit millimètre dans chacune des quatre directions, pour aboutir à un entrechoquement, un recouvrement brutal des carrés. Comme si souvent, je suis revenue au minimal, au presque rien, à l'à peine perceptible.
Pourquoi avoir choisi les deux couleurs jaunes ?
Je ne saurais le dire ; j'avais simplement une « envie jaune ».

Vera Molnar, 1998.

- **Étude géométrique de l'œuvre**

Le tableau est composé de 100 carrés disposés en grille de 10 par 10. Leur positionnement est déterminé par deux translations, l'une de vecteur $n\vec{i}$, l'autre de vecteur $m\vec{j}$, où n et m sont deux nombres entiers choisis de manière aléatoire entre -1 et 1.

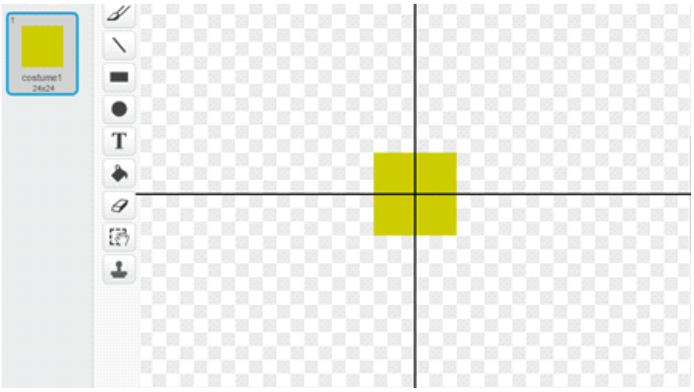
…/…

retour au sommaire

- **Programmation avec Scratch**

✓ **Le lutin**

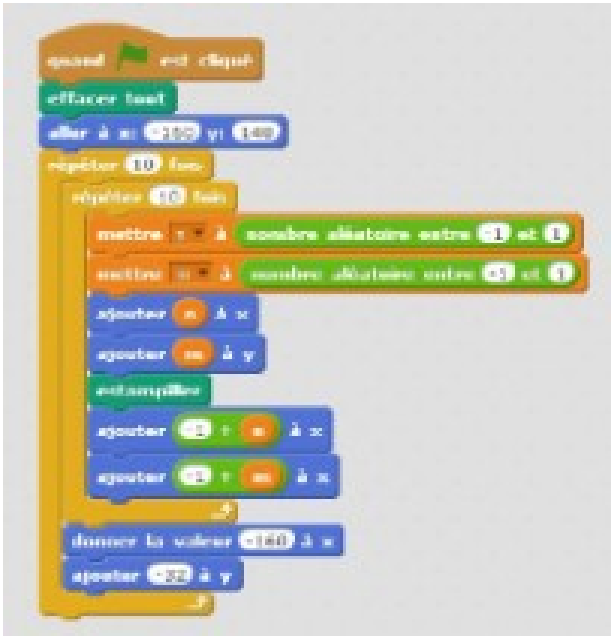
Il faut créer un lutin carré de côté 24 et placer le stylo sur son centre.



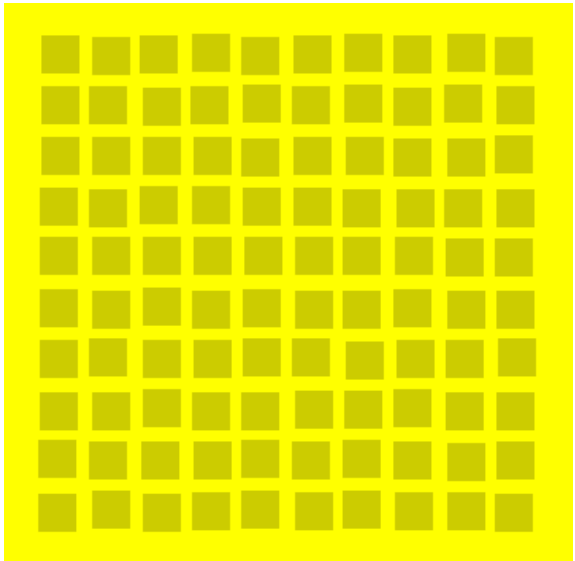
✓ **Le programme**

Les carrés appartenant à une ligne sont disposés tous les 32 pas. Pour déplacer chaque carré de manière aléatoire, il faut ajouter aux coordonnées de son centre un nombre aléatoire compris entre -1 et 1. Les coordonnées sont de la forme $n + x$ et $m + y$ avec n et m deux entiers compris entre -1 et 1.

La position de chaque carré doit être indépendante de celle des autres, il faut donc remettre le stylo de Scratch à sa position initiale avant de passer au carré suivant.



Reproduction aléatoire avec Scratch



retour au sommaire

La figure obtenue avec le programme ci-dessus n'est pas celle réalisée par Véra Molnar puisque la construction fait appel à un paramètre aléatoire.

La probabilité de réaliser la même figure que celle de l'œuvre est de $\frac{1}{9^{100}}$.

De plus, la variation des couleurs n'a pas été utilisée.

Eléments de sitographie

http://www.discip.ac-caen.fr/aca/reseaudegaleries/catalogue20032004/0.htm pour retrouver l'image de l'œuvre

http://www.discip.ac-caen.fr/aca/actu/frac_PREVIEUX.pdf pour retrouver ce que Vera Molnar dit en 1998 à propos de « 100 carrés jaunes »

http://www.matmutpourlesarts.fr/expositions/presse/vera-molnar-retrospective.pdf le dossier de presse d'une rétrospective 1942/2012. On y trouve le cheminement de la pensée de l'artiste pendant cette période.

http://www.veramolnar.com/blog/wp-content/uploads/VB2002_De_la_couleur_jaune.pdf On y trouve des dessins préparatoires et des réflexions à propos des cent couleurs jaunes utilisées.

On peut retrouver une œuvre de Véra Molnar actuellement au Grand Palais à Paris.

Pour de plus amples renseignements :

https://www.grandpalais.fr/fr/evenement/artistes-robots

https://www.grandpalais.fr/pdf/Dossier_Pedagogique_ARTISTESetROBOTS.pdf

retour au sommaire

ÉLÉMENTS DE GÉOMÉTRIE, DE CLAUDE CLAIRAUT

Clairaut avait écrit cet ouvrage à son retour de Laponie (où il était parti pour mesurer la longueur d'un méridien) à l'intention de son élève, la MARQUISE DU CHÂTELET.
Nous reproduisons ici la préface de ces éléments. L'auteur y dévoile ses principes pédagogiques afin de permettre aux « commençants » de développer leur « l'esprit d'invention ». Voilà qui pourrait nous inspirer...

PRÉFACE


ELEMENS
DE
GEOMETRIE
A PARIS,
M. DCC. XLI.

Quoique la Géométrie soit par elle-même abstraite, il faut avouer cependant que les difficultés qu'éprouvent ceux qui commencent à s'y appliquer, viennent le plus souvent de la manière dont elle est enseignée dans les éléments ordinaires. On y débute toujours par un grand nombre de définitions, de demandes, d'axiomes et de principes préliminaires, qui semblent ne promettre rien que du sec au lecteur. Les propositions qui viennent ensuite, ne fixant point l'esprit sur des objets plus intéressants, et étant par ailleurs difficiles à concevoir, il arrive communément que les commençants se fatiguent et se rebutent avant d'avoir aucune idée distincte de ce qu'on voulait enseigner.

Il est vrai que, pour sauver cette sécheresse naturellement attachée à l'étude de la Géométrie, quelques auteurs ont imaginé de mettre, à la suite de chaque proposition essentielle, l'image qu'on peut en faire pour la pratique ; mais par là ils prouvent l'utilité de la Géométrie, sans faciliter beaucoup les moyens de l'apprendre. Car chaque proposition venant toujours avant son usage, l'esprit ne revient à des idées sensibles qu'après avoir essuyé la fatigue de saisir des idées abstraites.

La mesure des terrains m'a paru ce qu'il y avait de plus propre à faire naître les premières propositions de Géométrie ; et c'est en effet l'origine de cette science, puisque Géométrie signifie *mesure de terrain*. Quelques auteurs prétendent que les Égyptiens, voyant continuellement les bornes de leurs héritages détruites par les débordements du Nil, jetèrent les premiers fondements de la Géométrie, en cherchant les moyens de s'assurer exactement de la situation, de l'étendue et de la figure de leurs domaines. Mais quand on ne s'en rapporterait pas à ces auteurs, du moins ne saurait-on douter que, dès les premiers temps, les hommes n'aient cherché des méthodes pour mesurer et partager leurs terres. Voulant dans la suite perfectionner ces méthodes, les recherches particulières les conduisirent peu à peu à des méthodes générales ; et s'étant enfin proposé de connaître le rapport exact de toutes sortes de grandeurs, ils formèrent une science d'un objet beaucoup plus vaste que celui qu'ils avaient d'abord embrassé, et à laquelle ils conservèrent cependant le nom qu'ils lui avaient donné dans son origine.

Afin de suivre dans cet ouvrage une route semblable à celle de ses inventeurs, je m'attache d'abord à faire découvrir aux commençants les principes dont peut dépendre la simple mesure des terrains et des distances accessibles ou inaccessibles, etc. De là, je passe à d'autres recherches qui ont une telle analogie avec les premières, que la curiosité naturelle à tous les hommes les porte à s'y arrêter ; et justifiant ensuite cette curiosité par quelques applications utiles, je parviens à faire parcourir tout ce que la Géométrie élémentaire a de plus intéressant.

On ne saurait disconvenir, ce me semble, que cette méthode ne soit au moins propre à encourager ceux qui pourraient être rebutés par la sécheresse de vérités géométriques dénuées d'applications ; mais j'espère qu'elle aura encore une utilité plus importante, c'est qu'elle accoutumera à chercher et à découvrir ; car j'évite avec soin de donner aucune

retour au sommaire

proposition sous la forme de théorème, c'est-à-dire de ces propositions où l'on démontre que telle ou telle vérité est, sans faire voir comment on est parvenu à la découvrir.

Si les premiers auteurs de mathématiques ont présenté leurs découvertes en théorèmes, ça a été sans doute pour donner un air plus merveilleux à leurs productions, ou pour éviter la peine de reprendre la suite des idées qui les avaient conduits dans leurs recherches. Quoi qu'il en soit, il m'a paru beaucoup plus à propos d'occuper continuellement mes lecteurs à résoudre des problèmes, c'est à dire chercher les moyens de faire quelque opération ou de découvrir quelque vérité inconnue, en déterminant le rapport qui est entre des grandeurs données et des grandeurs inconnues qu'on se propose de trouver. En suivant cette voie, les commençants aperçoivent, à chaque pas qu'on leur fait faire, la raison qui détermine l'inventeur ; et par là, ils peuvent plus facilement acquérir l'esprit d'invention.

On me reprochera peut-être, en quelques endroits de ces éléments, de m'en rapporter trop au témoignage des yeux, et de ne m'attacher pas assez à l'exactitude rigoureuse des démonstrations. Je prie ceux qui pourraient me faire un pareil reproche, d'observer que je ne passe légèrement que sur les propositions dont la vérité se découvre, pour peu qu'on y fasse attention. J'en use de la sorte, surtout dans les commencements, où il se rencontre plus souvent des propositions de ce genre, parce que j'ai remarqué que ceux qui avaient de la disposition à la Géométrie, se plaisaient à exercer un peu leur esprit ; et qu'au contraire ils se rebutaient lorsqu'on les accablait de démonstrations pour ainsi dire inutiles.

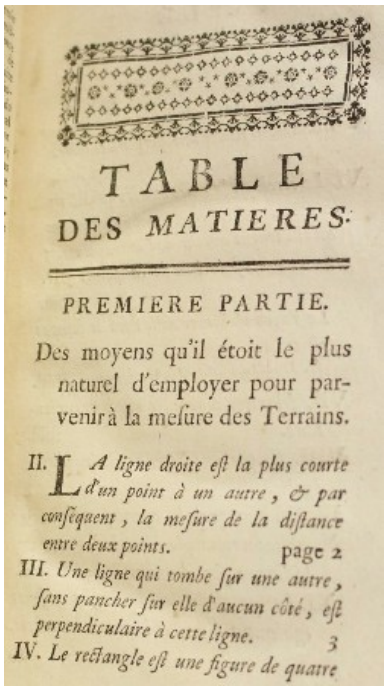


TABLE
DES MATIERES.

PREMIERE PARTIE.

Des moyens qu'il étoit le plus naturel d'employer pour parvenir à la mesure des Terrains.

II. La ligne droite est la plus courte d'un point à un autre, & par conséquent, la mesure de la distance entre deux points. page 2

III. Une ligne qui tombe sur une autre, sans pancher sur elle d'aucun côté, est perpendiculaire à cette ligne. 3

IV. Le rectangle est une figure de quatre

Qu'Euclide se donne la peine de démontrer que deux cercles qui se coupent n'ont pas le même centre, qu'un triangle renfermé dans un autre a la somme de ses côtés plus petite que celle des côtés du riangle dans lequel il est renfermé, on n'en sera pas surpris. Ce géomètre avait à convaincre des sophistes obstinés, qui se faisaient gloire de se refuser aux vérités les plus évidentes ; il fallait donc qu'alors la Géométrie eût, comme la logique, le secours des raisonnements en forme, pour fermer la bouche à la chicane. Mais les choses ont changé de face. Tout raisonnement qui tombe sur ce que le bon sens seul décide d'avance, est aujourd'hui en pure perte, et n'est propre qu'à obscurcir la vérité et à dégoûter les lecteurs.

Un autre reproche qu'on pourrait me faire, ce serait d'avoir omis différentes propositions qui trouvent leur place dans les éléments ordinaires, et de me contenter, lorsque je traite des propositions, d'en donner seulement les principes fondamentaux.

À cela je réponds qu'on trouve dans ce traité tout ce qui peut servir à remplir mon projet, que les propositions que je néglige sont celles qui ne peuvent être d'aucune utilité par elles-mêmes, et qui d'ailleurs ne sauraient contribuer à faciliter l'intelligence de celles dont il importe d'être instruit ; qu'à l'égard des propositions, ce que j'en dis doit suffire pour faire entendre les propositions élémentaires qui les supposent. C'est une manière que je traiterai plus à fond dans les éléments d'Algèbre, que je donnerai par la suite.

Enfin, comme j'ai choisi la mesure des terrains pour intéresser les commençants, ne dois-je pas craindre qu'on ne confonde ces éléments avec les traités ordinaires d'arpentage ? Cette pensée ne peut venir qu'à ceux qui ne considèrent pas que la mesure des terrains n'est point le véritable objet de ce livre, mais qu'elle me sert seulement d'occasion pour faire découvrir les principales vérités géométriques. J'aurais pu de même remonter à ces vérités, en faisant l'histoire de la physique, de l'astronomie ou de toute autre partie des mathématiques que j'aurais voulu choisir ; mais alors la multitude des idées étrangères, dont il aurait fallu s'occuper, aurait comme étouffé les idées géométriques, auxquelles seules je devais fixer l'esprit du lecteur.

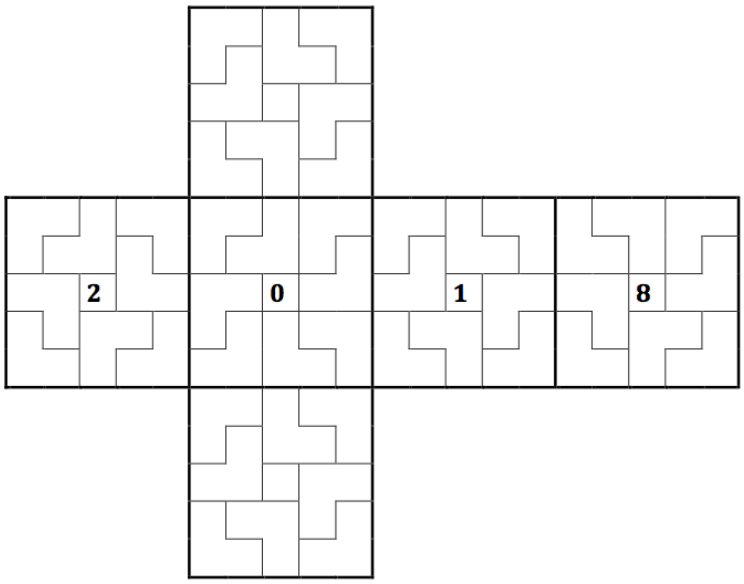
retour au sommaire

François DROUIN

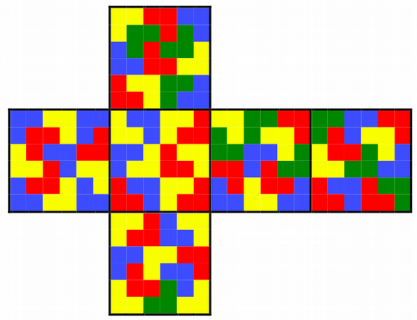
DES PATRONS ET DES « PETITS L »

Un patron à colorier pour l'an 2018

Avec le minimum de couleurs possibles, colorie le cube dont voici un patron. Deux zones voisines ne peuvent pas être de la même couleur.
En observant le patron, apparaissent des petits carrés au centre des faces contenant pour quatre d'entre eux les chiffres 2, 0, 1, 8 du nombre 2018. Pourrais-tu de plus obtenir ce minimum en coloriant les six petits carrés d'une même couleur?



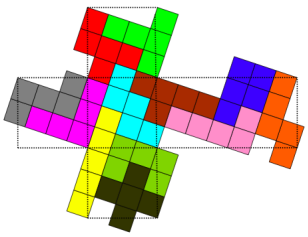
Ce défi a circulé en début d'année. Serait-il possible de n'utiliser que des « Petits L » pour recouvrir un patron de cube ?



Dans le Petit Vert n°124 (page 63), il est dit : « Avoir un côté multiple de 3 et au moins égal à 6 » caractérise donc les carrés recouvrables par des « Petits L ». De tels carrés pourront être les faces d'un cube.

L'exemple ci-contre a été imaginé par Arnaud Gazagnes (APMEP Groupe Jeux et Maths).

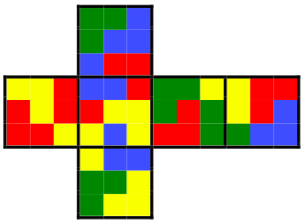
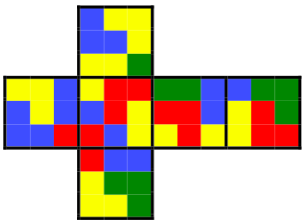
Arnaud préférait que les « Petits L » ne soient pas à cheval sur plusieurs faces. Martin Gardner a fait un autre choix lorsque il a imaginé ce recouvrement d'un cube par les douze pentaminos.



Ce qui est présenté dans la suite de cet article ne suit pas nécessairement les préoccupations d'Arnaud.

http://abarothsworld.com/Puzzles/Polyominoes/Pentomino%20Cubes.htm présente des recouvrements de cubes avec des pentaminos identiques pouvant être sur plusieurs faces.
http://abarothsworld.com/Puzzles/Polyominoes/Polyomino%20Cubes.htm présente des recouvrements cubes par des polyminos identiques : deux exemples utilisent des Petits L.

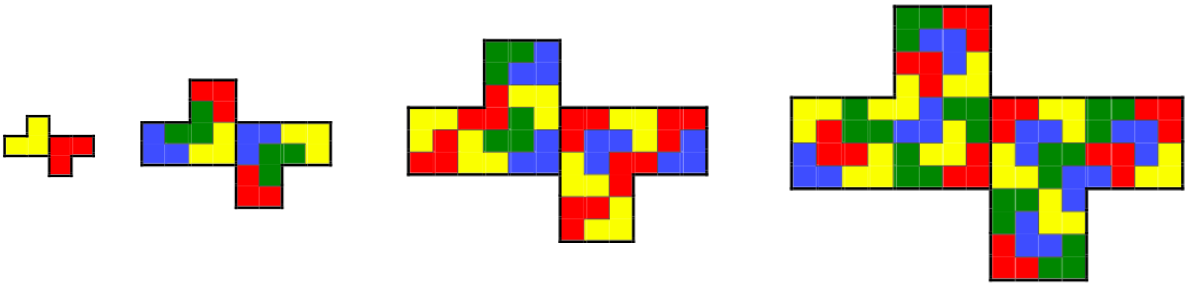
retour au sommaire

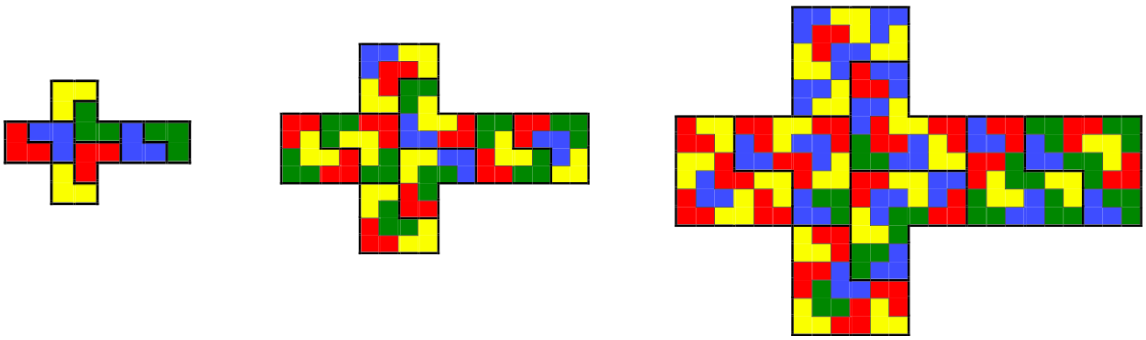
Les faces sont des carrés 3×3, des « Petits L » seront pliés lorsque le cube sera construit.

Des familles de patrons

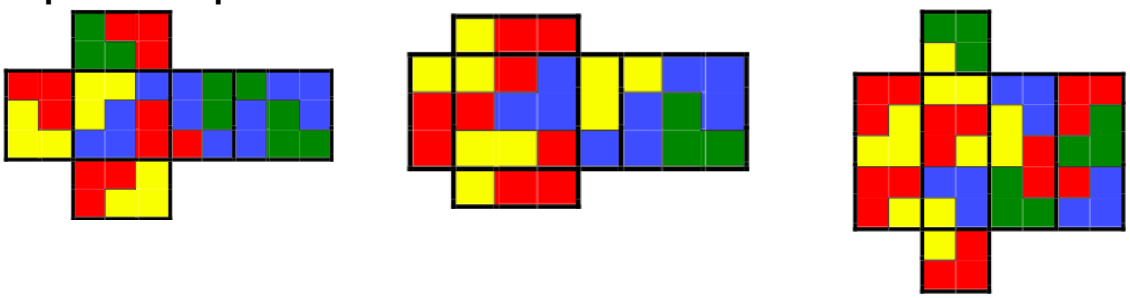
Une première famille de patrons de cubes recouverts par des « Petits L »



Une deuxième famille de patrons de cubes recouverts par des « Petits L »

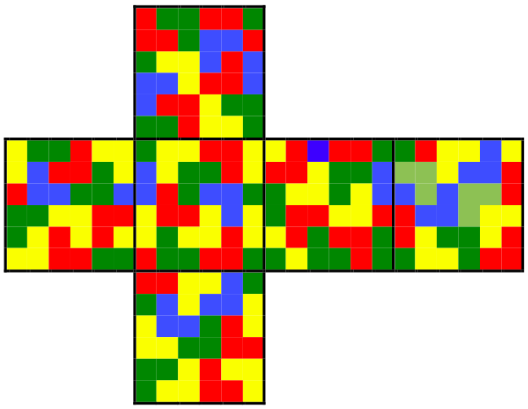


Des patrons de pavés



Remarque : il est possible de recouvrir des patrons de pavés dont aucune dimension n'est un multiple de 3.

Avec des élèves

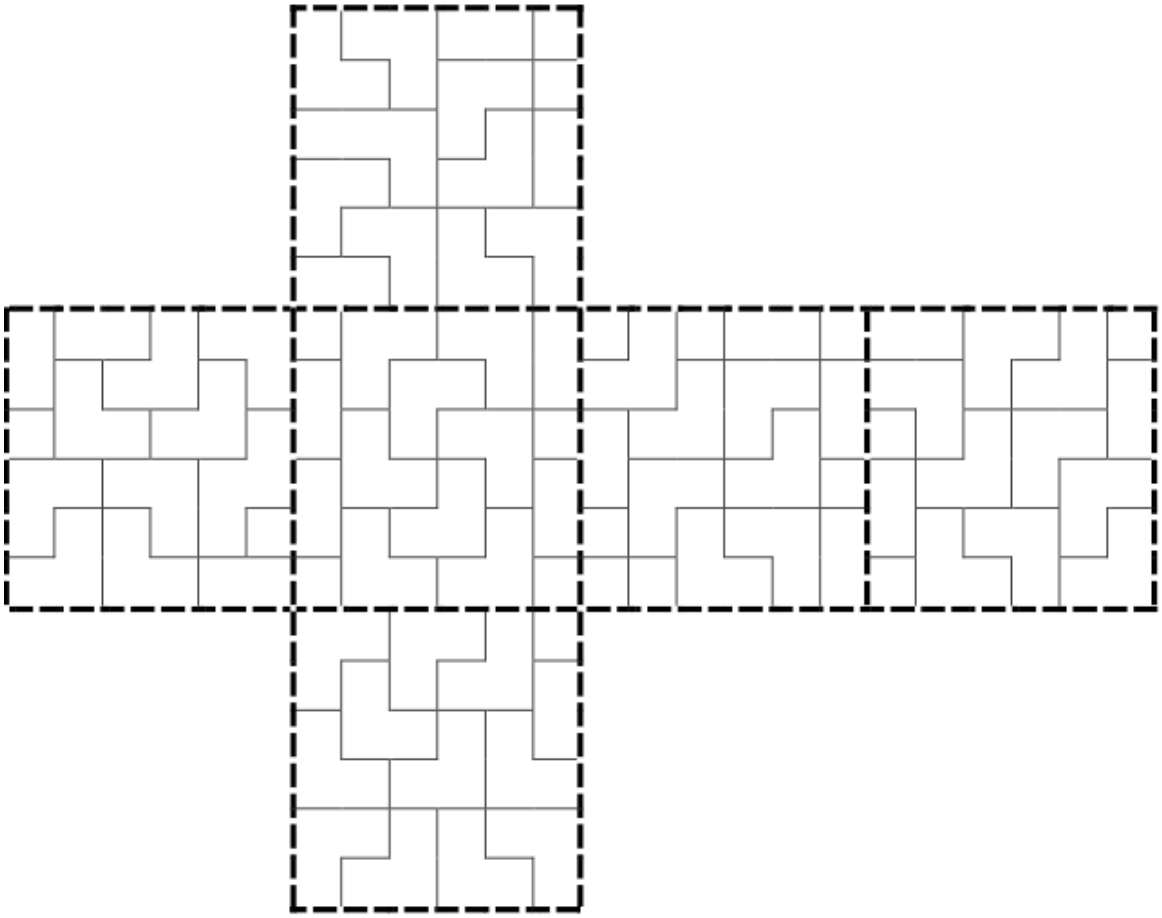


Lorsque le cube sera construit, certains « Petits L » seront pliés. Deux « Petits L » de même couleur ne peuvent avoir au maximum qu'un sommet en commun.

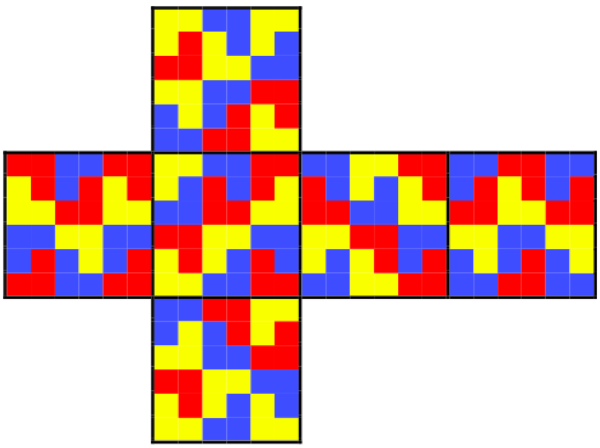
Réussirez-vous à colorier le recouvrement de ce patron de cube 6×6×6 en utilisant moins de cinq couleurs ?

retour au sommaire

Le patron à colorier



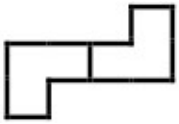
Moins de quatre couleurs ?



Ce patron de cube a été recouvert par des « Petits L » de trois couleurs seulement.

Pourrait-il en être de même pour les patrons de pavés et de cubes coloriés des deux pages précédentes ?

Une autre famille de patrons de cubes



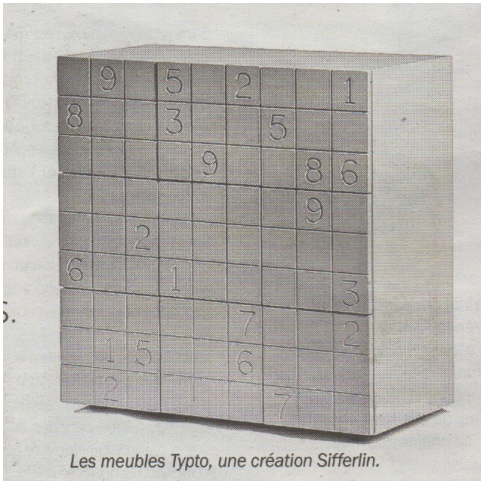
Deux « Petits L » recouvrent un patron de cube. Des dessins aux échelles 2, 3, 4 seront le début d'une autre famille de patrons de cubes à recouvrir par des « Petits L ».

retour au sommaire

UN MEUBLE SUDOKU

Groupe Maths & Jeux - APMEP Lorraine

« Le MAG », le supplément de l'Est Républicain du 25 février, présente un reportage à propos d'un créateur qui fait de bien belles choses.



Le meuble présenté dans « le MAG »

En allant sur le site du créateur
http://www.sifferlin.com/page/16/

La grille à résoudre

	9		5		2			1
8			3			5		
				9			8	6
							9	
		2						
6			1					3
					7			2
	1	5			6			
	2					7		

retour au sommaire

	9	6	5	8	2		7	1
8			3	6		5	2	9
2	5		7	9			8	6
							9	
		2						
6			1					3
	6				7			2
7	1	5			6			
	2			1		7	6	

La recherche se heurte assez rapidement à des choix à faire.

4	9	6	5	8	2	3	7	1
8	7	1	3	6	4	5	2	9
2	5	3	7	9	1	4	8	6
1	3	7	2	4	5	6	9	8
5	8	2	6	3	9	1	4	7
6	4	9	1	7	8	2	5	3
3	6	4	8	5	7	9	1	2
7	1	5	9	2	6	8	3	4
9	2	8	4	1	3	7	6	5

Une première joueuse lorraine a tenté de dépasser ces choix à faire et arrive à une solution double (les chiffres bleus peuvent être permutés).

3	9	6	5	8	2	4	7	1
8	7	4	3	6	1	5	2	9
2	5	1	7	9	4	3	8	6
1	3	7	6	2	5	8	9	4
5	8	2	6	4	9	6	1	7
6	4	9	1	7	8	2	5	3
9	6	8	4	5	7	1	3	2
7	1	5	2	3	6	9	4	8
4	2	3	8	1	9	7	6	5

3	9	6	5	8	2	4	7	1
8	4	7	3	6	1	5	2	9
2	5	1	7	9	4	3	8	6
1	8	4	2	3	5	6	9	7
5	3	2	6	7	9	1	4	8
6	7	9	1	4	8	2	5	3
9	6	3	4	5	7	8	1	2
7	1	5	8	2	6	9	3	4
4	2	8	9	1	3	7	6	5

Une autre joueuse lorraine nous fournit une solution dans laquelle des chiffres **bleus** peuvent être permutés pour de nouvelles solutions et une autre bien différente de celle présentée précédemment. Le créateur de ce sympathique mobilier n'est sans doute pas au courant de l'unicité de solution défendue par les amateurs de ce type de grille ; il a cependant fourni de bons moments de recherche à des joueuses et joueurs de Lorraine. Nous conseillons cependant aux acheteurs et à leur entourage de ne pas chercher remplir le Sudoku directement sur le meuble !

retour au sommaire

MATH & MEDIA

Merci à tous nos lecteurs qui alimentent cette rubrique. Qu'ils continuent à le faire, en nous envoyant si possible les originaux, et aussi - et surtout - les commentaires ou activités possibles en classe que cela leur suggère.

Envois par la poste à Jacques VERDIER (7 rue des Bouvreuils, 54710 FLEVILLE) ou par courrier électronique : jacverdier@orange.fr .

Les archives de cette rubrique seront bientôt disponibles sur notre nouveau site àl'adresse : www.apmeplorraine.fr

TROIS EUROS 50 OU 3,50 EUROS ?

Une petite pépite retrouvée dans le Nouvel Observateur n°1749 du 14 mai 1998, à propos de l'écriture des nombres décimaux. C'est Delfeil de Ton qui écrit au sujet du prix d'un tableau de Van Gogh qui serait peut être un faux, qu'il ne vaudrait pas des millions, pas même trois euros cinquante. Dans sa rubrique, il a fait imprimer « **3 euros 50** ». Voici ce qu'il nous dit...

« J'ai fait imprimer trois euros cinquante. Je suis allé voir les correcteurs du journal et je leur ai demandé de ne pas me corriger, de ne pas me faire écrire 3,50 euros. Je lisais un article dans un quotidien, l'autre jour : *Si Napoléon mesurait 1,59 mètre, De Gaulle plafonnait à 1,95 mètre*. Il faut lire, bien sûr, 1 mètre 59 et 1 mètre 95. Alors pourquoi nous force-t-on à écrire 1,93 mètres ? C'est pas du français, ça. On dirait un anglicisme, je ne sais si c'en est un. En tout cas c'est une règle idiote, une complication inutile. Pour arriver à cette écriture illogique, qui heurte le rythme de la langue, il faut ajouter une virgule dont on n'aurait aucun besoin si on écrivait normalement. Pourquoi qu'on se laisse faire ? Parce que les Français sont des veaux, comme dirait l'autre qui mesurait un virgule quatre-vingt-treize mètre ? ».

Cet extrait figure également dans la brochure "Des décimaux en classe de sixième", publié par l'IREM de Lorraine. Elle est téléchargeable.

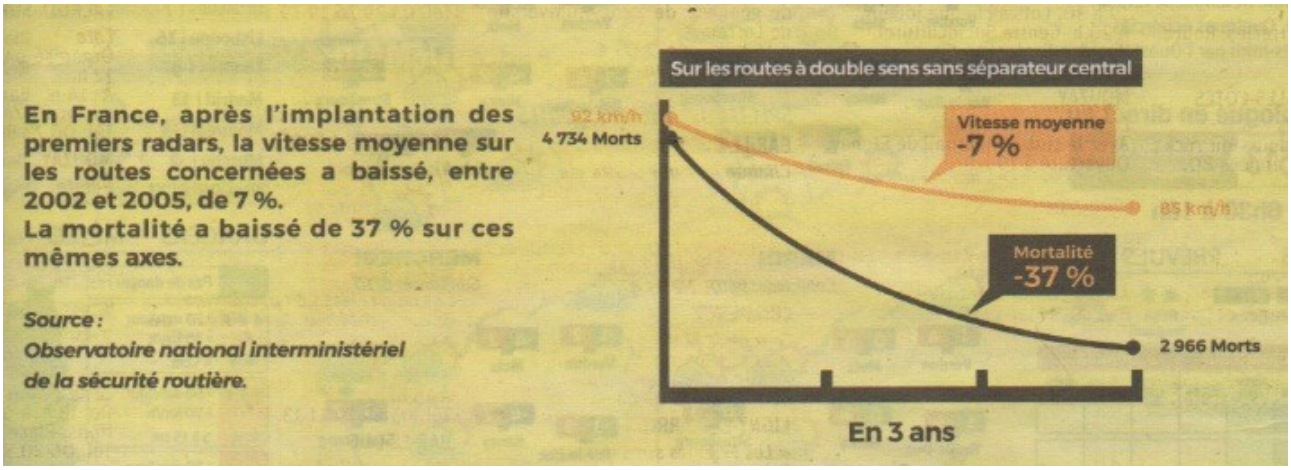
https://www.dailymotion.com/video/x1dfywh

retour au sommaire

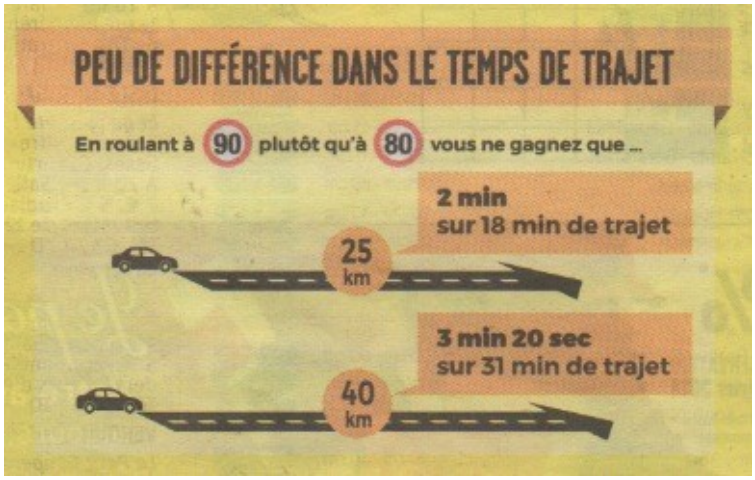
AU 1er JUILLET 2018

À compter du 1er juillet 2018 la vitesse maximale autorisée sur les routes à double sens sans séparateur central sera imitée à 80 km/h.
Cette information nous est précisée sur des pages entières de nos quotidiens. Cette décision fait suite à la conclusion d'une enquête menée à la demande du Conseil national de la sécurité routière.
« Baisser la vitesse de 10 km /h sur les routes à double sens sans séparateur pourrait permettre de sauver 350 à 400 vies chaque année ». Si la formulation « aurait pu sauver » avait été utilisée, nous aurions pensé que ces 350 à 400 décès ont eu lors d'accidents à des vitesses comprises entre 80 et 90 km /h. Le conditionnel est utilisé, la lecture de la page 9 du rapport nous indique que ce chiffrage a été obtenu suite à une « modélisation résultant des expériences internationales de modification de vitesse maximale autorisée ».

Dans nos quotidiens, des infographies illustrent le propos.



Entre les années 2002 et 2005, le citoyen lecteur imagine les années 2003 et 2004 mais observe trois années représentées sur le graphique par trois intervalles. Les courbes oranges et noire continues ont-elles pour but de montrer l'évolution du nombre de morts mois après mois ? Le point d'intersection entre les deux axes n'est pas l'origine des valeurs numériques utilisées en ordonnée, accentuant les baisses visualisées.



La vitesse moyenne de 92 km/h à propos des 4 734 morts peut surprendre, et passer d'une vitesse moyenne 92 km/h à une vitesse moyenne de 85 km/h correspond à une baisse de 7,6% qui aurait pu être arrondie à 8%.

Cette autre infographie (ci-contre) pourrait devenir un support d'activité en classe pour faire recalculer les gains annoncés.

retour au sommaire

UN DODÉCAÈDRE RÉGULIER « POP-UP »[1]

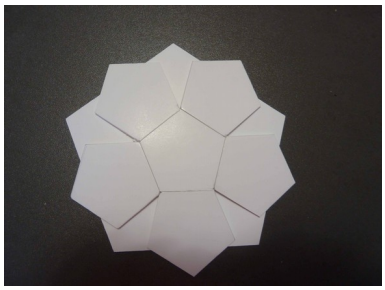
par Walter Nurdin

Le dodécaèdre régulier est le seul solide de Platon à faces pentagonales régulières.
Il a, comme son nom le précise, 12 faces qui sont des pentagones réguliers.
Chaque pentagone ayant 5 côtés et comme chaque arête est commune à deux pentagones le nombre total d'arêtes est $\frac{12\times5}{2}$ = 30 arêtes.

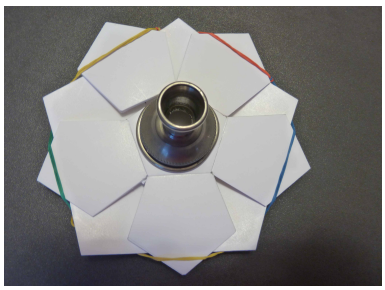
Comme chaque sommet est commun à 3 pentagones on obtient $\frac{12\times5}{3}$ = 20 sommets.

La formule d'Euler est bien vérifiée (faces + sommets - arêtes = 2) puisque : 12+20-30 = 2.

Pour réaliser un dodécaèdre régulier « pop-up » on découpe une feuille de carton (ou de carton plume) pour obtenir deux exemplaires du modèle dessiné en annexe 1.
Une fois la découpe effectuée on marque les plis pour qu'ils soient bien souples. Avec du carton plume, une entaille sur la surface du dessus suffit.
Les pentagones vont tenir par la feuille inférieure qui couvre le carton plume.
On place les deux découpes l'une sur l'autre en ayant effectué une rotation de $\frac{\pi}{5}$ pour l'une des pièces (voir ci-dessous).



Puis on fait passer un élastique alternativement par-dessus l'un des pentagones du « demi » patron du dessus, puis par-dessous le pentagone voisin du « demi » patron du dessous, tout en maintenant fermement avec un doigt les découpages à plat.



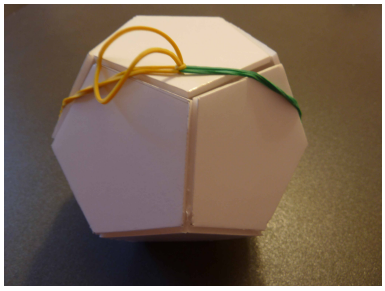
N.B. L'objet au centre est posé là pour que la construction « ne se relève pas ».

Enlevez votre doigt et vous allez voir se dresser le dodécaèdre régulier.
Il peut être transporté à plat avec l'élastique et reconstruit à volonté.
La difficulté est de choisir le (les) bon(s) élastique(s) et le bon carton correspondant.
Pour réaliser le modèle photographié on peut utiliser du carton plume mousse de 3 mm et 5 élastiques reliés entre eux.

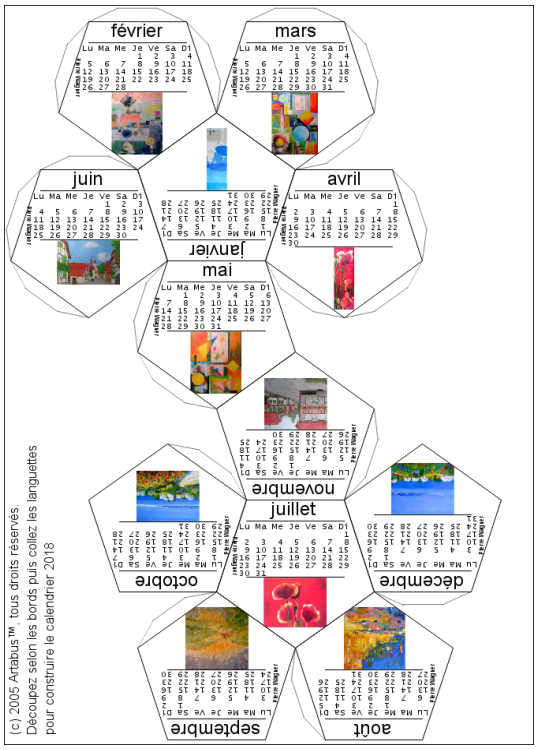
[1] Tiré de « Mon cabinet de curiosités mathématiques » de Ian Stewart.

retour au sommaire

En prenant les précautions d'usage, le modèle construit peut être de nouveau aplati et mis dans une chemise avec rabat et élastique. Le dodécaèdre reprendra sa forme lorsqu'on ouvrira délicatement la pochette.



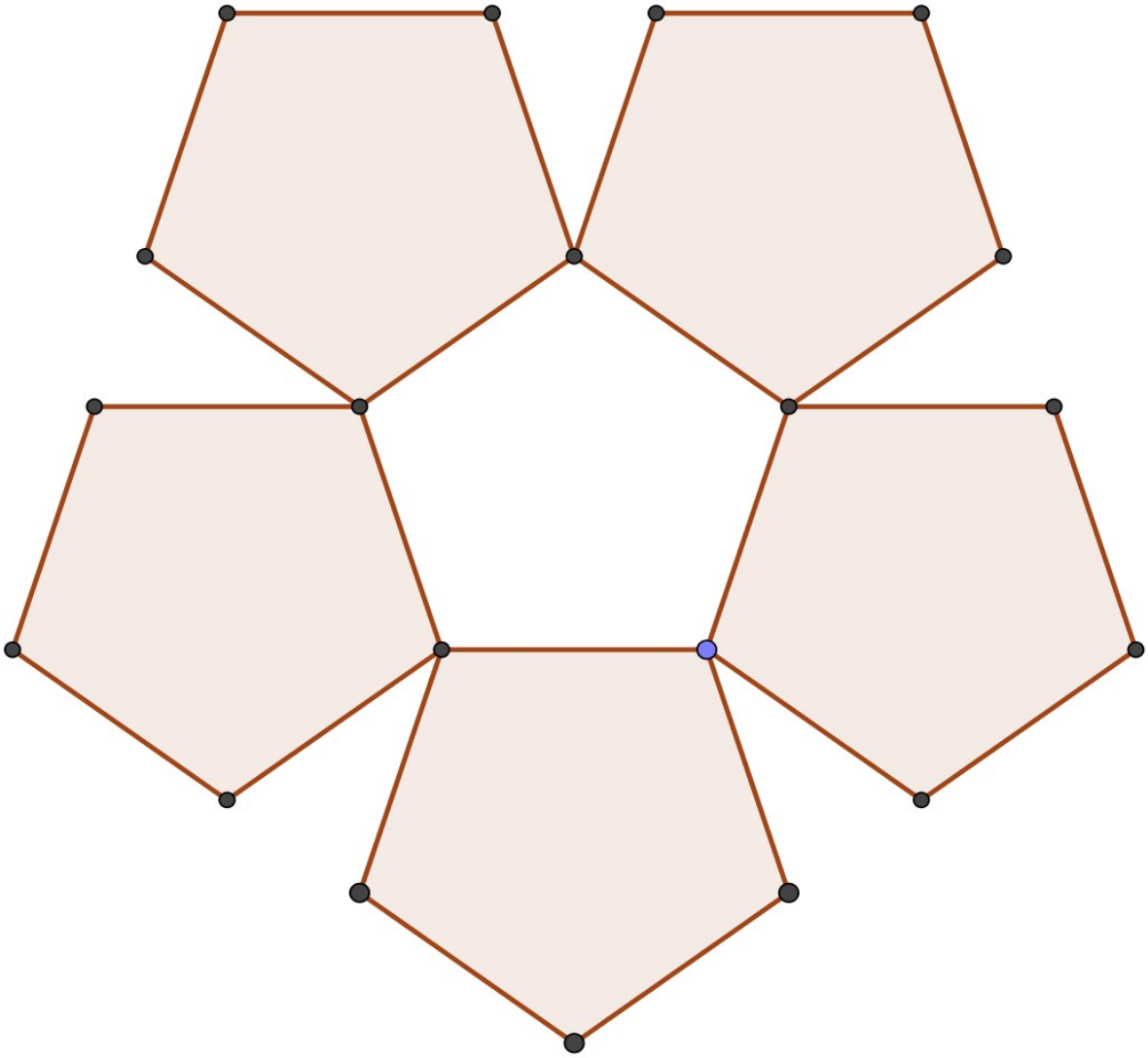
Si maintenant vous voulez réaliser un calendrier 2018 vous pouvez pour chaque mois utiliser l'une des 12 faces du dodécaèdre régulier.
Le site « Artabus », d'une galerie d'art en ligne, le permet et agrémente chaque mois d'une œuvre artistique (voir ci-dessous).



Voir annexe, page suivante

retour au sommaire

ANNEXE



Un autre site permet la réalisation d'un calendrier sur un dodécaèdre régulier et sur un dodécaèdre rhombique (ce solide sera évoqué dans un futur Petit Vert).

Arts et dodécaèdres

En 1955, Dali a utilisé un dodécaèdre dans son œuvre Le sacrement de la dernière Cène. Les rencontres avec le nombre d'or sont nombreuses. Le site académique de Poitiers nous présente une étude mathématique du tableau.

En 1943, Escher a utilisé un dodécaèdre dans son œuvre « reptiles ». Thérèse Éveilleau a utilisé ce dessin pour un puzzle à manipuler.

Vers 1500, dans le « Portrait de Luca Pacioli » attribué à Jacopo' de Barbari, un dodécaèdre est représenté en bas et à droite de la toile.

N'oublions pas les dodécaèdres galloromains évoqués dans le Petit Vert n°130 (page 57).

retour au sommaire

DES DÉFIS POUR NOS ÉLÈVES

SOLUTION DU DÉFI LES 3 OURS (PV133)

Rappel de l'énoncé. Trois ours prennent leur petit déjeuner. Le père prend la moitié des pots de miel qui sont sur la table, plus un. La mère prend la moitié de ce qui reste plus un pot. Le petit ours prend lui aussi la moitié de ce qui reste plus un pot. Il ne reste alors plus rien sur la table. Combien y avait-il de pots sur la table avant le petit déjeuner ?

Solution. Soit n le nombre de pots au début.

Le père prend $\frac{n}{2}+1$ pots, il en reste donc $\frac{n-2}{2}$.

La mère prend $\frac{n-2}{4}+1$ pots, il en restera donc $\frac{n-6}{4}$.

Le petit ours prend alors $\frac{n-6}{8}+1=\frac{n+2}{8}$ pots, et il reste $\frac{n-6}{4}-\frac{n+2}{8}=\frac{n-14}{8}$ pots, qui doit être égal à 0. Le nombre initial de pots était donc **n = 14**.

Remarque. Ce défi est à mettre en parallèle avec le défi du Petit Vert n°128, « Le diable et le fainéant ». Outre la solution algébrique, il était fourni une solution numérique et une feuille de calculs. Elles pourront être source d'inspiration pour écrire une solution autre que celle présentée ci-dessus.

Les mathématiques sont une gymnastique de l'esprit et une préparation à la philosophie.

Isocrate

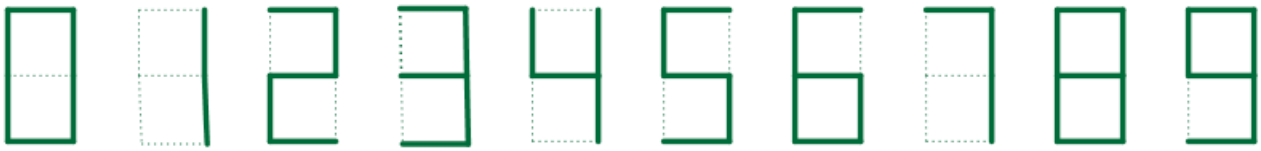
ANNONCE

Dans le numéro 101 du Petit Vert (mars 2010), nous avions publié un article intitulé « **Les nombres de 10 à 100, étude de quelques "anomalies"** ». Faute de place dans notre petit bulletin, nous n'avions pas pu publier les 7 pages d'annexes de cet article.
Vous pouvez désormais retrouver, à cette adresse, la totalité de l'article et ses annexes.
Nous vous souhaitons bonne lecture.

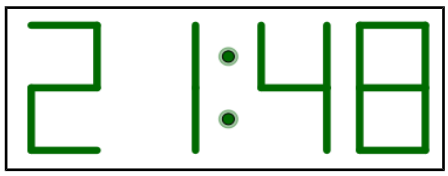
retour au sommaire

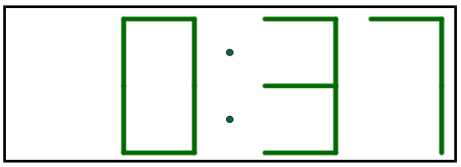
SOLUTION DU DÉFI « LE RÉVEIL-MATIN » (PV 133)

Un réveil-matin affiche les chiffres grâce à des diodes luminescentes. Pour chaque chiffre, de deux à sept diodes sont utilisées : par exemple, le chiffre "1" utilise deux diodes, le chiffre "8" en utilise sept (voir image ci-dessous).



L'affichage du réveil comporte d'une part les heures, d'autre part les minutes, ces deux nombres étant séparés par un double point, comme le montrent les deux exemples ci-dessous, le premier correspondant à 21 h 48 et le second à 0 h 37.





On remarquera que, tant qu'on n'arrive pas à la dixième heure, le réveil n'affiche pas le chiffre des dizaines d'heure (on lit 0 h 37 et non pas 00 h 37).

Le défi est le suivant :

❶ dans un cycle de 24 heures (de 0 h 00 à 23 h 59), combien de fois l'affichage présentera-t-il un centre de symétrie, et à quels moments cela aura-t-il lieu,

❷ combien de fois l'affichage présentera-t-il un axe de symétrie vertical, et à quels moments cela aura-t-il lieu,

❸ combien de fois l'affichage présentera-t-il un axe de symétrie horizontal, et à quels moments cela aura-t-il lieu ?

Éléments de solution

❶ Les seuls chiffres qui peuvent être utilisés ici sont 0, 2, 5, 8 (qui sont « autosymétiques »), ainsi que 6 et 9 (chacun étant symétrique de l'autre). Attention : le 1 ne peut pas être utilisé, car il est « décalé » vers la droite.
Par ailleurs, pour les heures avant 10 heures, il n'y a qu'un seul chiffre affiché à gauche, ce qui ne permet pas un affichage symétrique.

Les seules possibilités sont donc, pour les heures, 20 et 22.

Il n'y a ainsi que deux réponses valides pour cette question ❶ : **20h02** et **22h22**.

❷ Pour cette seconde question, les seuls chiffres utilisables sont 0, 2 et 8.

Comme pour la question précédente, aucune heure avant 22 heures ne peut être utilisée.

Là encore, il n'y a que deux possibilités pour la question ❷ : **20h05** et **22h55**.

❸ Pour cette dernière question, les seuls chiffres utilisables sont 0, 1, 3 et 8.

Par contre, il est maintenant possible d'utiliser les heures depuis 0 heure.

La partie gauche de l'affichage (les heures) peut donc être 0, 1, 3, 8, 10, 11, 13, 18.

La partie droite (les minutes) peut être 00, 01, 03, 08, 10, 11, 13, 18, 30, 31, 33 ou 38.

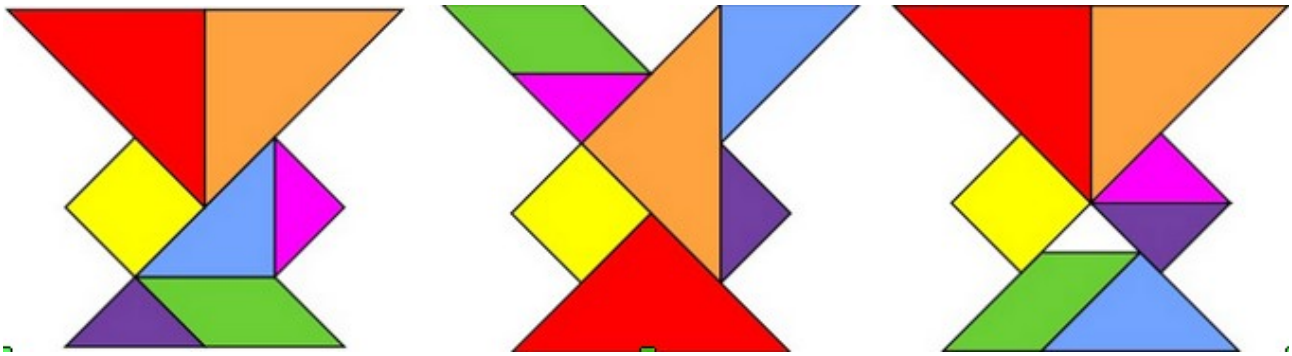
Cela fait **96 possibilités**. Voir le tableau ci-après.

retour au sommaire

h\min	0	1	3	8	10	11	13	18	30	31	33	38
0	0h00	0h01	0h03	0h08	0h10	0h11	0h13	0h18	0h30	0h31	0h33	0h38
1	1h00	1h01	1h03	1h08	1h10	1h11	1h13	1h18	1h30	1h31	1h33	1h38
3	3h00	3h01	3h03	3h08	3h10	3h11	3h13	3h18	3h30	3h31	3h33	3h38
8	8h00	8h01	8h03	8h08	8h10	8h11	8h13	8h18	8h30	8h31	8h33	8h38
10	10h00	10h01	10h03	10h08	10h10	10h11	10h13	18h18	10h30	10h31	10h33	10h38
11	11h00	11h01	11h03	11h08	11h10	11h11	11h13	11h18	11h30	11h31	11h33	11h38
13	13h00	13h01	13h03	13h08	13h10	13h11	13h13	13h18	13h30	13h31	13h33	13h38
18	18h00	18h01	18h03	18h08	18h10	18h11	18h13	18h18	18h30	18h31	18h33	18h38

SOLUTION DU DÉFI « LES TROIS VASES » (PV 133)

Les 7 pièces du puzzle qui ont servi à représenter les trois vases.



En prenant comme hypothèse que le carré initial avec lequel on a construit les puzzles des trois vases est de 4 unités, on peut calculer, par exemple, la hauteur des trois vases.

Le premier vase a une hauteur de $2+\sqrt{2}+2$ unités, le second vase une hauteur de 5 unités, et le troisième (celui avec un trou) une hauteur de $\frac{7\sqrt{2}}{2}$ unités.

La différence de hauteur de ces trois vases est quasi imperceptible, seul le calcul exact des hauteurs permet de démasquer la « supercherie ».

*****

DÉFI 134-a : « 1/2018 »

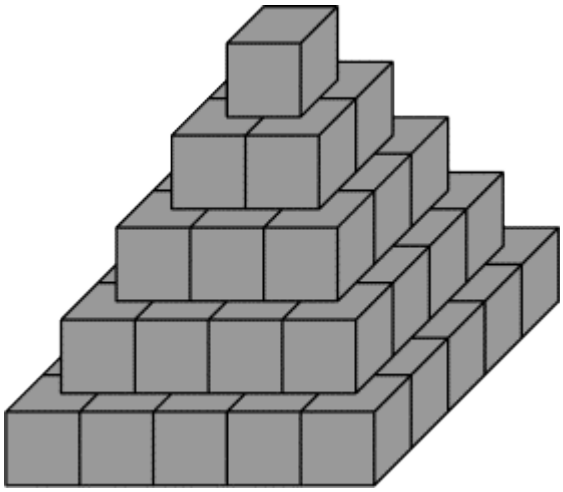
Trouver deux nombres entiers **a** et **b** (avec **a** ≠ **b**) tels que $\frac{1}{a}+\frac{1}{b}=\frac{1}{2018}$.

Si possible, donner **toutes** les solutions.

retour au sommaire

DÉFI 134-b : PYRAMIDE

La pyramide ci-dessous est une version simplifiée d'une pyramide Maya, dite également « pyramide à degrés » (les degrés sont des marches d'escalier). Elle est formée de blocs cubiques ayant tous la même dimension.



Combien a-t-on utilisé de cubes pour construire cette pyramide de 5 étages ? Combien en faudrait-il pour construire une pyramide de 10 étages ? De 20 étages ? De *n* étages ?
On dispose d'une boite de 1000 cubes. Combien d'étages (complets) pourra-t-on construire ?

Tous les cubes de cette pyramide visibles de l'extérieur sont gris, mais tous ceux qui sont à l'intérieur sont blancs.
Combien de cubes blancs et combien de cube gris faut-il pour construire une pyramide de 10 étages ? De *n* étages ?

Notre photo, la pyramide Maya de Teotihuacan

Pour en savoir plus sur les pyramides à degrés :
https://fr.wikipedia.org/wiki/Pyramide_%C3%A0_degr%C3%A9s

retour au sommaire

MATh.en.JEANS

Le 29ème congrès pour le Grand Est, la Belgique et le Luxembourg et un lycée roumain (jumelé avec un lycée belge), s'est tenu les 23 et 24 mars 2018 à la Faculté des sciences et de technologie de Vandœuvre. Les 380 élèves de collège et lycée, accompagnés de 57 enseignants et 29 chercheurs, ont présenté leurs travaux sous forme d'exposés ou/et d'animations dans leur stand. Ils ont aussi assisté à des conférences et participé à des réunions.

Les mines réjouies durant ces deux journées traduisaient l'enthousiasme et le plaisir de faire des maths en les vivant, pas en les subissant.
Encore un congrès très réussi !

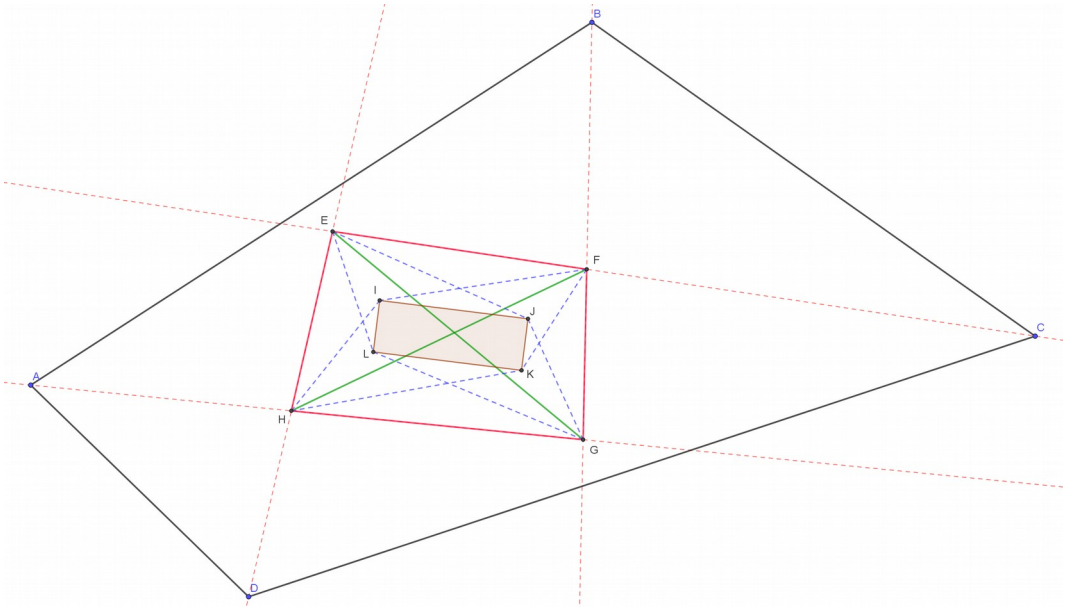
Pour de plus amples informations https://www.mathenjeans.fr/Congres2018
Et si l'aventure vous tente, n'hésitez pas et contactez Louisette.Hiriart@ac-nancy-metz.fr

retour au sommaire

DES PROBLÈMES POUR LE PROF

INDICATIONS POUR LE PROBLÈME n°133

« C'est plié » : problème proposé par Damien Mégy



Rappelons l'énoncé

Le quadrilatère ABCD est quelconque.
Les droites « rouges » sont les bissectrices des angles de ce quadrilatère.
Leurs points d'intersection définissent un quadrilatère EFGH.
Les droites « bleues » sont des bissectrices des triangles définis par les segments diagonaux [EG] et [FH] et les quatre sommets du quadrilatère EFGH. Leurs intersections définissent un quadrilatère IJKL.

Quelle est la nature du quadrilatère IJKL ?

Personne n'ayant proposé de réponse, nous vous proposons quelques pistes pour la résolution de ce problème. La solution complète sera proposée dans le prochain Petit Vert.

Indications

La démonstration s'établit en trois étapes :

- dans un premier temps, on montre que les points E, F, G et H sont cocycliques,
- dans un second temps, on exprime une relation entre, par exemple, $\left(\overrightarrow{LH}, \overrightarrow{LG}\right)$ et $\left(\overrightarrow{EH}, \overrightarrow{EG}\right)$
- on montre enfin que le quadrilatère IJKL est rectangle en prouvant que les angles sont droits.

ÉNONCÉ DU PROBLÈME n°134

Proposé par Jacques Verdier

On se donne une suite de n entiers u_1, u_2, … , u_n. J'affirme qu'on peut trouver k termes consécutifs de cette suite, dont la somme est divisible par n. Vrai ou faux ?

Le responsable de cette rubrique est philippe.fevotte@wanadoo.fr.
Lui envoyer vos propositions de solutions à ces deux problèmes (nous espérons en avoir une grande quantité), ainsi que toute proposition de nouveau problème.

retour au sommaire

SOLUTION DU SOPHISME DU TRIMESTRE (n°133)

LE PLUS GRAND NOMBRE ENTIER EST 1

Pour le démontrer, nous majorons les entiers non nuls en utilisant une contraposition.

Soit un entier positif A > 1. Alors en multipliant par A, $A^2 > A$. Nous avons donc trouvé un entier A^2 plus grand que A : cela signifie que A n'est pas le plus grand entier.

On a donc montré que si A > 1, alors A n'est pas le plus grand entier. En contraposant, on en déduit que le plus grand entier est 1. Ainsi, 1 est plus grand que tous les nombres entiers.

Solution

Bien sûr, il y a une erreur quelque part dans notre raisonnement : nous savons tous que 1 n'est pas le plus grand nombre entier ! Nous allons débusquer l'erreur de raisonnement.

La première partie du raisonnement est correcte, ainsi que sa conclusion : il est effectivement vrai que « Si A dépasse 1, alors A n'est pas le plus grand entier ». Le problème est dans la contraposition. Dans le texte ci-dessus, on a fait un raccourci : la vraie contraposée de ce qui précède est « Si A est le plus grand entier, alors A ne dépasse pas 1 (c'est à dire A =1) ». Il y a un **SI** au début de cette phrase.

Lisez bien : cette phrase ne signifie pas, contrairement à ce qui est écrit dans la « fausse démonstration », que 1 est le plus grand entier (ce que l'on devrait démontrer avant de conclure), alors cet entier serait nécessairement 1. Encore aurait-il fallu montrer, au préalable, qu'il existait bien un plus grand entier … ce qui risque d'être difficile !

On peut même conclure, in fine, qu'il n'y a pas de plus grand entier, puisqu'il y a au moins un entier plus grand que 1 (par exemple 2).

Sophisme extrait de http://maths.amatheurs.fr

LE SOPHISME DU TRIMESTRE (n°134)

La définition du dictionnaire Robert est la suivante : « *Argument, raisonnement faux malgré une apparence de vérité* ». Le Petit Vert vous proposera régulièrement des sophismes, comme celui qui suit. Envoyez toute nouvelle proposition à jacverdier@orange.fr.

Affirmation : *n* points quelconques d'un plan sont toujours alignés

Cette démonstration se fait par récurrence.

Commençons par montrer « *l'hérédité* » : supposons qu'on ait montré que n points sont alignés. Soient $(n+1)$ points : A_1, A_2, …, A_{n+1}. Les points de A_1 jusqu'à A_n sont un ensemble de n points donc, d'après l'hypothèse de récurrence, ils sont alignés. Autrement dit, le point A_1 est sur la droite formée par les points de A_2 à A_n.

De même, les points A_2 jusqu'à A_{n+1} forment un ensemble de points donc, d'après l'hypothèse de récurrence, ils sont alignés. Donc le point A_{n+1} est sur la droite formée par les points A_2 à A_n. Les $(n+1)$ points sont alignés.

Puisqu'on a « l'hérédité », il ne nous manque que l'initialisation de la récurrence. Or elle est évidente : pour $n = 2$, les deux points sont toujours alignés !

Donc, finalement, par récurrence, pour tout n à partir de 2, n points du plan sont toujours alignés !

retour au sommaire