AVRIL 2021 | VOLUME 5 | NUMÉRO 3

L'AXIOMATIQUE

COMMENT GÉNÉRER DES NOMBRES PSEUDO-ALÉATOIRES?

LES PSEUDO-MATHÉMATIQUES ET CEUX QUI LES FONT

LE MOIS DE MARS AU CLUBMATH

RAMANUJAN

CONJECTURES ET PREUVES

GRATUIT

AXIOMATIQUE

| LE MOT DE LA RÉDACTION

BONJOUR À TOI!

Eh oui, c'est déjà la dernière édition de la session d'hiver 2021. Ne t'en fais pas le journal sera de retour dès la session d'automne. D'ailleurs, si tu veux participer au comité l'an prochain, tu peux nous écrire quand tu le veux. Aussi, si tu veux simplement écrire sur un sujet dans une seule édition, il n'y a pas de problème! En plus, nous avons une grande nouvelle pour toi :

Le Journal L'Axiomatique deviendra officiellement le journal de L'ENSEMBLE des étudiantes et étudiants en mathématiques et statistique à l'Université de Montréal!

Donc, oui, toi qui es aux cycles supérieurs et qui aimerais dont écrire ce qui t'intéresses, tu vas pouvoir participer aussi! Ceci implique, entre autre, que le journal aura maintenant 16 pages (actuellement 12). C'est l'un des effets de la pandémie visiblement, la prise de poids!

Au plaisir de vous revoir l'an prochain, profitez de votre été!

PIERRE-OLIVIER PRUD'HOMME,
RÉDACTEUR EN CHEF

FAÉCUM

CETTE ÉDITION EST RÉALISÉE GRÂCE À L'APPUI FINANCIER REÇU DE **LA FÉDÉRATION DES ASSOCIATIONS ÉTUDIANTES DU CAMPUS DE L'UNIVERSITÉ DE MONTRÉAL**

L'ÉQUIPE DE L'AXIOMATIQUE

RÉDACTEUR EN CHEF
PIERRE-OLIVIER PRUD'HOMME

RUBRIQUE DE L'AEMSUM
SHOPHIKA VAITHYANATHASARMA

GRAPHISTE ET METTEUR EN PAGE
LEON CARLOS NAVARRO CAMPILLO

CHRONIQUEURS ET CHRONIQUEUSES
BÉATRICE HAJJAR
JULIEN HÉBERT-DOUTRELOUX
MATHIEU PINEAULT
ÉLOI MARTIN
SIMON LUANGXAY
ANNE CLÉROUX

POUR NOUS JOINDRE

COURRIEL
LAXIOMATIQUE@GMAIL.COM

SITE WEB
LAXIOMATIQUE.COM

FACEBOOK
FACEBOOK.COM/LAXIOMATIQUE

PROCHAINE PARUTION

OCTOBRE 2021

| SOMMAIRE

UN MOIS D'AVRIL REVIGORANT

Le mois d'avril est arrivé et, avec lui, l'odeur de la liberté estivale. Bien que la fin de session approche à grand pas, j'espère que vous vous laisserez tenter par cet appel à quelques occasions. Car s'il est important d'étudier, il demeure que l'air frais revigore l'esprit et apaise l'âme. Mais surtout, en cette période d'isolement, laissez-vous le temps de parler avec vos ami.e.s et vos camarades. Seul.e ou en gang, n'hésitez pas à utiliser le Discord de Maths-Stat ou encore à venir à l'un de nos nouveaux rendez-vous hebdomadaires : les soirées Harry Potter du vendredi soir. Si le temps et la santé publique nous le permettent, il nous fera plaisir de vous voir en grand nombre dans certains parcs des environs, anciens comme nouveaux ! Je vous souhaite au nom de l'AEMSUM la meilleure des fins de session!

LAURENT ALSÈNE-RACICOT, PRÉSIDENT
DE L'AEMSUM

TOUT LE MONDE À BORD!

Où vont les gens après le bacc? Selon la légende, ce n'est pas bien long avant qu'ils prennent le large. Certains partent à la conquête du marché du travail. Certains se réorientent d'abord à bâbord ou à tribord. D'autres partent plutôt à la dérive pour s'intégrer à de nouveaux cycles marins, à des cycles supérieurs. Ils sont ainsi une centaine de matelots, carburant à l'eau claire et au jus de cafetière. Pour poursuivre leur parcours ils doivent suivre de nouveaux cours, les écouler avant que ceux-ci ne les coulent. Ils sont en rédaction, en stage, à la recherche. À la recherche de quoi donc? De la perle noire, de l'anneau parfait ou de la chaîne de Markov, qu'importe. Ils cherchent à trouver, voilà tout, mais la plupart du temps se trouvent à chercher.

Quelle part de vérité portent ces récits? Dès l'an prochain, vous en aurez le cœur net. Car dès l'an prochain, les cycles supérieurs se joindront au valeureux équipage de *L'Axiomatique*. Dès l'an prochain, vous pourrez les voir en chair et en prose. À bas les légendes urbaines, tous les cycles seront désormais unis par la plume. À bas les murs mitoyens, nous cohabiterons dorénavant dans les pages de ce convivial journal. Quelle grande nouvelle! Après tout, ne sommes-nous pas tous issus de la même famille *aisenstadtienne*? Descendants de la même lignée mathématico-statisticienne? Après tout, ne sommes-nous pas dans le même bateau?

PHILIPPE ROBITAILLE-GROU, PRÉSIDENT
DE L'AECSMS

ON EST LÀ POUR VOUS

La rubrique *On est là pour vous* a pour but de partager des ressources de toutes sortes pour venir en aide aux étudiant.e.s qui vivent des situations difficiles de tous types. Ce mois-ci, nous vous présentons des ressources d'aide à la réussite scolaire.

Si vous avez lu l'édition de Décembre 2020, dans l'entrevue avec Mme Véronique Hussin, il a été brièvement question du Service d'appui à la formation interdisciplinaire et à la réussite étudiante (SAFIRE). Le SAFIRE a plusieurs mandats dont celui de la réussite étudiante. En effet, ce service offre aux étudiant.e.s des conseils concernant leur cheminement universitaire et lors de changements de programme. Il met en place aussi les mesures d'accommodement accordées aux étudiant.e.s en situation de handicap.

Le service de Soutien aux étudiants en situation de handicap est le service qui pourra vous aider si vous êtes en difficulté en raison d'une condition médicale. Pour les contacter, vous devez remplir un formulaire en ligne et prendre rendez-vous par téléphone. Voici, le lien : http://www.bsesh.umontreal.ca/accueil/index.htm. Si vous n'avez pas de conditions particulières, mais que vous êtes en difficulté, vous pouvez contacter Denis Béliveau, conseiller en réussite étudiante, par courriel. Il pourra vous référer aux bonnes ressources et vous accompagner dans l'élaboration d'un plan d'action pour remettre votre réussite sur pied. Son courriel : denis.beliveau@umontreal.ca.

L'Université de Montréal offre aussi des services d'aide par l'entremise du Centre étudiant de soutien à la réussite (CÉSAR). En effet, en plus d'offrir des ressources d'aide psychologique, le CÉSAR offre un service de consultation individuelle pour vous soutenir dans vos apprentissages ainsi qu'un service de consultation éclair pour répondre à vos questions urgentes entourant le nouveau contexte d'études. D'ailleurs, si vous n'êtes toujours pas familier ou à l'aise avec les plateformes d'apprentissage mises en place, un guide se trouve à l'adresse suivante : https://www.cesar.umontreal.ca/apprentissage/index.htm.

Évidemment, plusieurs services de tutorat peuvent aussi vous venir en aide. D'ailleurs, le Département de mathématiques et statistique met aussi à votre disposition, moyennant des frais, un service de tutorat. Sur ce site , https://dms.umontreal.ca/fr/research/seminars/92-club-mathematique, vous trouverez une liste de tuteurs et tutrices qui pourront vous aider en fonction des cours dans lesquels vous avez davantage de difficulté. D'autres services peuvent aussi vous venir en aide. Par exemple, Carré d'As Tutorat offre un service de tutorat privé et Blitz 4.0 offre en plus des cours intensifs. (https://carredastutorat.com/tutorat-universitaire/ et https://blitztutorat.com/, respectivement leur adresse web)

Bref, plusieurs services sont mis à votre disposition, donc n'hésitez pas à les utiliser : ils sont là pour vous!

PIERRE-OLIVIER PRUD'HOMME,
ÉTUDIANT EN ACTUARIAT

| CLUBMATH DE L'UNIVERSITÉ DE MONTRÉAL

LE MOIS DE MARS AU CLUBMATH

Les amateurs et amatrices de mathématiques ont été choyés ces derniers temps puisque le mois de mars a été chargé au Clubmath. Depuis le retour de la relâche, des conférences intéressantes ont été présentées chaque semaine et voici un petit récapitulatif de celles-ci.

Le mois de mars a bien débuté avec une présentation de Simon St-Amant, ancien étudiant de l'UdeM qui est désormais au doctorat en Mathématiques de l'Information à l'Université de Cambridge. Dans celle-ci, il nous a parlé des mathématiques derrière les rayons X en plongeant dans le monde de la géométrie intégrale. Ensuite, il s'est attaqué au sujet plus général de ce qu'on appelle les problèmes inverses qui consiste comme leur nom l'indique, à inverser un opérateur pour retrouver un objet initial. Un cas encore plus intéressant à étudier de ceux-ci est lorsqu' un certain bruit est ajouté au problème. Retrouver l'objet original peut être particulièrement difficile dans ces situations, mais le conférencier nous a appris que parfois le bruit peut même nous aider. Parmi les exemples de problèmes inverses nommés dans la conférence, on compte le « débruitage » d'une image, la dissipation de la chaleur et la tomographie par impédance électrique. Puis, le conférencier a conclu en présentant les diverses approches pour résoudre ceux-ci.

La semaine suivante, le Clubmath a eu une audience record de 140 participants réunis dans une seule conférence sur Zoom. Parmi les spectateurs, il y avait des étudiants du baccalauréat, des cycles supérieurs, des professeurs et même des gens d'autres universités. Vous vous demandez sans doute alors qui était l'invité tant attendu qui a présenté le 17 mars. En fait, nous n'avons reçu la visite de nul autre que le professeur James Maynard de l'Université d'Oxford. Ce mathématicien qui a notamment été un chercheur postdoctoral au CRM et qui est renommé pour ses travaux en théorie des nombres analytique nous a présenté une conférence décontractée intitulée Patterns in the primes. Dans celle-ci, Maynard s'est penché sur quelques questions entourant les problèmes ouverts posés par Landau en 1912 qui sont la conjecture de Goldbach, la conjecture des nombres premiers jumeaux, la conjecture de Legendre et le problème de n2+1. Au cours de la conférence, il a répondu à trois questions principales qui sont « pourquoi s'intéresser à ces problèmes? », « pourquoi sommes-nous si mauvais à les prouver? » et « pourquoi sommes-nous si certains de leur réponse si nous ne pouvons pas les prouver? ». La présentation a touché différents sujets comme le dernier théorème de Fermat, le cryptage de données, les « safe prime », la fonction zêta de Riemann et bien plus encore! Cet exposé captivant a eu lieu grâce aux efforts combinés du comité organisateur du Clubmath, du professeur Dimitris Koukoulopoulos et bien sûr grâce à la participation de notre invité James Maynard.

Pour ce qui est de la dernière conférence du mois, elle n'a pas encore été présentée au moment d'écrire ces lignes, mais lorsque vous les lirez elle aura déjà eu lieu. Pour finir le mois, nous avons reçu Guillaume Roy-Fortin, diplômé du DMS qui est à ce jour, maître d'enseignement en mathématiques à l'École de technologie supérieure (ÉTS). Sa dernière visite au Clubmath remonte à l'automne 2018 où il avait parlé de géométrie intégrale. Cette fois-ci, sa présentation portait sur un sujet différent qui était l'apprentissage profond géométrique. Dans celle-ci, il a défini les réseaux de convolution géométrique.

Enfin, il reste deux dernières conférences pour le mois d'avril et vous ne voudrez surtout pas les manquer. Nous espérons vous voir en grand nombre à celles-ci. Comme d'habitude, les exposés des dernières semaines sont déjà disponibles sur notre chaine YouTube et dans nos archives, vous pourrez donc les écouter et réécouter comme bon vous semble! Comme cet article est notre dernier de la session hiver 2021, l'équipe du Clubmath vous souhaite une bonne fin de session et beaucoup de succès dans vos évaluations!

MATHIEU PINEAULT, AU NOM DU COMITÉ ORGANISATEUR DU CLUBMATH

SOLUTION AU JEU MATHÉMATIQUE

KENDOKU À LA PAGE 10

7+ 5	2	3÷ 6	4÷ 4	1	11+ 3
4÷ 4	1	2	6÷ 6	3	5
14+ 6	5	3	1	2÷ 4	2
5+ 2	3	20× 4	5	5- 6	1
12× 3	4	1	7+ 2	5	24× 6
1	1- 6	5	5+ 3	2	4

KENDOKU À LA PAGE 10

SOLUTION AU JEU MATHÉMATIQUE

RAMANUJAN

DES THÉORÈMES À PARTIR DE CONSTANTES PLUTÔT QUE DE VARIABLES?

Des scientifiques en Israël ont développé un ordinateur qui serait capable de générer des conjectures, ces pré-théorèmes qui ne demandent ensuite qu'à être prouvés par des mathématiciens. La «Ramanujan Machine», nommée d'après le célèbre mathématicien autodidacte Srinivasa Ramanujan, ferait en effet preuve d'une pensée originale qui permettrait de générer des conjectures complètement nouvelles. Ces conjectures, une fois démontrées, pourraient avoir de nombreuses applications en mathématique, mais aussi en physique, en informatique ou en ingénierie.

Puisque la machine ne prend pas en compte des facteurs comme la difficulté de prouver les conjectures qu'elle génère ou l'état d'avancement des mathématiques au moment où elle les génère. En effet, c'est sur des constantes célèbres, telles pi ou le nombre d'or, par exemple, que la «Ramanujan Machine» se base pour essayer de générer des conjectures.

Il s'agit là d'une approche qui n'a pas encore été beaucoup explorée en mathématiques, mais un peu plus dans les sciences expérimentales. De nombreuses formules en physique, par exemple, s'appuie sur des constantes, considérées comme les constantes fondamentales de l'univers. Les liens entre les constantes, ainsi que leur structure, demeurent une aire majoritairement inexplorée des mathématiques. Grâce à son intuition mathématique, la machine développée par des ingénieurs de l'institut israélien de Technion se propose d'explorer ces liens et cette structure.

L'invention a été nommée « Ramanujan machine » a été nommée après Srinivasa Ramanujan car ce dernier se distinguait par son intuition mathématique extraordinaire, qui provenait entre autres du fait qu'il était autodidacte. En se distinguant de l'avancement actuel des mathématiques à son époque (1887-1920), ce dernier utilisait, notamment, son propre système de notation. Son travail, à lui également, s'intéressait de près aux constantes telles que pi ou e. Srinivasa Ramanujan est, notamment, l'auteur de la sommation de Ramanujan et des nombres premiers de Ramanujan.

Selon son site officiel, ramanujanmachine.com, la machine de Ramanujan aurait déjà découvert plusieurs douzaines de nouvelles conjectures. Pour les intéressés, ces conjectures sont ouvertes à quiconque voudrait tenter de les prouver, et pourrait donc être nommées après vous si vous en trouvez la preuve!

ANNE CLÉROUX, ÉTUDIANTE AU BACCALAURÉAT EN MATHÉMATIQUES ET PHYSIQUE

$\sqrt{RAMANUDICANDE}$

Les motivations premières d'un article sont la recherche et le partage d'une question ainsi que de sa réponse. Ainsi, un corrigé a bien plus de valeur si les solutions sont données avec les énoncées. Cela est bien, mais cette rigueur n'a pas été utilisée par un certain Srinivasa Ramanujan assurément l'autodidacte le plus productif des 20 derniers siècles. Ce mathématicien de génie aura tout au long de sa carrière découvert pas moins de 3900 formules et théorèmes, mais la quasi-totalité est léguée sans démonstration. On nomme d'ailleurs les Cahiers de Ramanujan, les quatre recueils manuscrits dans lesquels se retrouvent ses résultats. L'histoire ne s'arrête pas à sa mort, car, plus de 50 ans après celle-ci, un autre mathématicien, Bruce Carl Berndt, s'intéresse de près à ses cahiers et consacrera plus de 20 ans à leurs éditions commentées. Ce dernier ainsi que ses collaborateurs, George Andrews, Richard Askey et Robert A. Rankinse, tenteront de prouver ou de retracer les références expliquant les résultats de Ramanujan. Maintenant, la question ayant poussé l'écriture du présent article est la suivante : est-il possible de prouver une des formules (aux allures spectaculaires) en utilisant des outils simples ? La formule est la suivante (présente sur la page Wikipédia consacrée à Ramanujan) :

Corollaire.

$$\sqrt{5+\sqrt{5+\sqrt{5-\sqrt{5+\sqrt{5+\sqrt{5+\cdots}}}}}} = \frac{2+\sqrt{5}+\sqrt{15-6\sqrt{5}}}{2}$$

où l'alternance des signes est périodique $(+,+,+,-,+)$.

Cette identité est en fait un corolaire de la proposition suivante :

Proposition (« Entry 32 »). Les inégalités suivantes :

$$x^2 = a + y$$
$$y^2 = a + z$$
$$z^2 = a + u$$
$$u^2 = a + x$$

détermine un polynôme en x (ou y ou z ou u) de degré 16. Ce polynôme peut-être factorisé en un produit de quatre polynômes quartiques, l'un d'entre eux est $x^4 - 2ax^2 - x + a^2 - a$. Les autres polynômes quartiques restants ont la forme

$$(x^2 + px + \frac{1}{2}(p^2 - 2a - 1/p))(x^2 + qx + \frac{1}{2}(q^2 - 2a - 1/q)), \quad (1)$$

où $pq = -1$ et $p + q$ sont une racine de l'équation polynomiale

$$z^3 + 3z = a(1 + az) \quad (2)$$

Démonstration : Direct. La preuve qui suivra est tirée du quatrième volume des ouvrages de Berndt.
Soit $\{a_n\}$ une suite de termes telle que $a_1 = \sqrt{5}, a_2 = \sqrt{5 + \sqrt{5}}, ...$ où a_n est le n^e radical imbriqué de la partie de droite du corollaire.
Maintenant, posons les fonctions f, g continues définies par

$$f(x) = \sqrt{5 + \sqrt{5 + \sqrt{5 - x}}} \quad \text{et} \quad g(x) = \sqrt{5 + x} \quad (0 \leq x \leq 5)$$

Remarquons que f est décroissante et que g est croissante sur leur interval de définition. En particulier,

$$\begin{aligned} f(0) = a_3 > f\left(\sqrt{5}\right) &= (f \circ g)(0) = a_4 > (f \circ g)\left(\sqrt{5}\right) \\ &= a_5 > (f \circ g)\left(\sqrt{5 + \sqrt{5}}\right) = a_6 > (f \circ g)(a_3) = a_7 \end{aligned}$$

et

$$\begin{aligned} a_7 < (f \circ g)(a_4) = a_8 < (f \circ g)(a_5) = a_9 &< (f \circ g)(a_6) \\ &= a_{10} < (f \circ g)(a_7) = a_{11} \end{aligned}$$

Il suit par induction que

$$\begin{cases} a_{8n+3} > a_{8n+4} > a_{8n+5} > a_{8n+6} > a_{8n+7} \\ a_{8n+7} < a_{8n+8} < a_{8n+9} < a_{8n+10} < a_{8n+11} \end{cases} \quad (3)$$

pour tout entier n non négatif. En prenant la racine carrée et puis en additionnant ou soustrayant 5, on montre aussi par induction que $2 < a_7 < a_{15} < a_{23} < \cdots < a_{8n+7} < a_{8n+11} < a_{8n+3} < \cdots < a_{19} < a_{11} < a_3 < 5$, pour tout entier n non négatif. Par conséquent, la sous-suite $\{a_{8n+7}\}$ est monotone croissante tandis que la sous-suite $\{a_{8n+3}\}$ est monotone décroissante. Toutes deux sont bornées, alors elle converge, et disons qu'elles convergent respectivement vers α et β. Notons que $a_{8n+7} = (f \circ g)(a_{8n+3})$. Par continuité de f et g

$$\begin{aligned} \lim_{n\to\infty} (f \circ g)(a_{8n+3}) &= (f \circ g)\left(\lim_{n\to\infty} a_{8n+3}\right) \\ &= (f \circ g)(\beta), \end{aligned}$$

alors que a_{8n+7} tend vers α lorsque $n \to \infty$. Aussi, puisque $a_{8n+11} = (f \circ g)(a_{8n+7})$, alors par un argument similaire, $\beta = (f \circ g)(\alpha)$.

Donc, $\beta = (f \circ g)(\beta)$. En posant la fonction $h = f \circ g$, alors on observe que α et β sont des points fixes de $h \circ h$, c'est-à-dire que $p(x) = x$ où dans ce cas $(h \circ h)(\alpha) = \alpha$ et $(h \circ h)(\beta) = \beta$. En dérivant $(h \circ h)$, on remarque $0 < (h \circ h)'(x) < 1$ pour $a_7 \leq x \leq a_3$. Ainsi, l'équation $(h \circ h)(x) = x$ a au plus une racine sur cet intervalle. Alors, $\alpha = \beta$ et donc la sous-suite $\{a_{4n+3}\}$ convergent.
Par (3), on peut aussi conclure que la suite $\{a_n\}$ converge.
en posant, $a = 5$ dans la suite d'équalité de la proposition présentée plus haute, on obtient

$$u^2 = 5 + x,$$
$$z^2 = 5 + u,$$
$$y^2 = 5 + z,$$
$$x^2 = 5 + y,$$

Que l'on peut combiner de sorte à obtenir l'équation polynomiale

$$5 + x = (((x^2 - 5)^2 - 5)^2 - 5)^2 \quad (4)$$

En posant, $F(x) = 5 + x - (((x^2 - 5)^2 - 5)^2 - 5)^2$ et en le factorisant par *Mathematica* on trouve

$$\begin{gathered} (x^2 - x - 5) \cdot (x^2 + x - 4) \cdot (x^4 - 4x^3 - 4x^2 + 31x - 29) \cdot \\ (x^8 + 4x^7 - 10x^6 - 54x^5 + 9x^4 + 226x^3 + 125x^2 - 301x - 269) \end{gathered}$$

Un monstre dont l'une des racines est la limite de $\{a_n\}$. Par la proposition, $p + q$ est une racine de (2)

$$z^3 - 17z - 4 = (z^2 - 4z - 1)(z + 4) = 0.$$

Soit $p + q = -4$. Alors, puisque $pq = -1$, on trouve que $p, q = -2 \pm \sqrt{5}$. Ainsi, le polynôme de l'équation (1) est donné par

$$\begin{aligned} &\left(x^2 + \left(-\sqrt{5} - 2\right)x + \frac{1}{2}\left(\left(-\sqrt{5} - 2\right)^2 - 10 - \frac{1}{-\sqrt{5} - 2}\right)\right) \cdot \\ &\left(x^2 + \left(\sqrt{5} - 2\right)x + \frac{1}{2}\left(\left(\sqrt{5} - 2\right)^2 - 10 - \frac{1}{\sqrt{5} - 2}\right)\right) = \\ &x^4 - 4x^3 - 4x^2 + 31x - 29 \end{aligned}$$

Les quatre racines de ce polynôme sont données par $\frac{2 \pm \sqrt{5} \pm \sqrt{15 - 6\sqrt{5}}}{2}$. Il ne reste plus qu'à montrer que $\frac{2 + \sqrt{5} + \sqrt{15 - 6\sqrt{5}}}{2}$ à l'expansion radicale donnée dans l'énoncé du corollaire. Cela peut se faire à l'aide de *Mathematica* en calculant les seize racines de $F(x)$ dont une seule satisfait l'équation requise (une variante de 4) :

$$(f \circ g)(x) = x = \sqrt{5 + \sqrt{5 + \sqrt{5 - \sqrt{5 + x}}}}$$

□

En outre la preuve a utilisé la convergence de suites ainsi que de sous-suites, la continuité, la différentiabilité, la définition de point fixe et le principe d'induction. L'utilisation de ces concepts est restée relativement simple, tout en montrant une identité biscornue. Évidemment, la preuve ne serait pas aussi directe sans l'entrée #32 dont la démonstration n'est pas plus difficile à comprendre malgré que travailler avec des polynômes de degré seize mène inévitablement à jongler avec de grandes équations.

JULIEN HÉBERT-DOUTRELOUX, ÉTUDIANT AU BACCALAURÉAT EN MATHÉMATIQUES PURES ET APPLIQUÉES

A alpha	B beta	C charlie	D delta	E echo	F foxtrot
G golf	H hotel	I india	J juliette	K kilo	L lima
M mike	N november	O oscar	P papa	Q quebec	R roméo
S sierra	T tango	U uniform	V victor	W whisky	X x-ray
Y yankee	Z zulu				

LES CODES DÉTECTEURS ET L'ISBN

En 1956, l'organisation de l'aviation civile internationale (OACI) commence à utiliser un alphabet phonétique afin d'éliminer un problème majeur dans la communication radio. En effet, les pilotes en mission ont des informations importantes à se transmettre et ne peuvent pas se permettre qu'un mot soit mal compris par leur interlocuteur. L'alphabet phonétique de l'OTAN, aussi appelé l'alphabet radio international, corrige ce problème en associant à chaque lettre un mot. Par exemple, au lieu de dire le mot *droite*, un pilote dirait : **D**elta **R**omeo **O**scar **I**ndia **T**ango **E**cho. Ce système standardisé permet d'extraire efficacement du message reçu le message d'origine. Avec la multiplication des moyens de communications numériques, la création de tels systèmes s'est accélérée. Ceux-ci doivent permettre de bien comprendre le message reçu malgré de possibles erreurs dans la transmission. Il sera donc question dans cet article des codes détecteurs et correcteurs, mais plus particulièrement de l'International standard book number (ISBN).

Dans cet article, l'information à communiquer sera désignée par un vecteur u dont toutes les coordonnées sont des caractères appartenant à une liste finie. Dans notre exemple où le mot transmis était *droite*, le vecteur u serait (d,r,o,i,t,e) et la i^e coordonnée, notée u_i, appartient à l'ensemble des 26 lettres de l'alphabet. Le vecteur u sera transformé selon un certain code et on enverra le vecteur v. Lors de la transmission, on fait l'hypothèse qu'au plus un v_i est altéré. Après cette possible altération due au médium de communication, l'interlocuteur reçoit le vecteur w. Il devra faire deux choses, la première est de vérifier si une erreur s'est glissée dans le vecteur w. L'explication des détails de cette étape seront faits plus loin pour l'exemple particulier de l'ISBN. La deuxième étape est de corriger l'erreur s'il y en a une. Ce que l'on nomme un code détecteur est un algorithme permettant de vérifier si une erreur a été commise. On l'appelle aussi un code correcteur si le receveur du message est capable de corriger le message erroné reçu.

Maintenant que l'hypothèse de base, au plus une altération possible, a été exposée et que le vocabulaire utilisé a été expliqué, l'exemple précis de l'ISBN sera décortiqué pour bien comprendre la mécanique d'un tel code. Bien que l'ISBN ne soit qu'un code détecteur et non correcteur, il est intéressant de démystifier la série de chiffres présente sur tous les manuels scolaires ou sur tous les autres livres. Ce numéro international normalisé du livre est constitué de 13 chiffres regroupés en cinq groupes et il permet l'indentification unique d'une édition d'un livre. Les parties sont de longueur variable et permettent de déterminer la région géographique, l'éditeur ainsi que l'édition particulière. Le dernier chiffre de la séquence est appelé la clé de contrôle et est utilisé dans la validation de l'ISBN.

Les détails associant à un livre son ISBN ne seront pas détaillés. Seulement la détermination du dernier caractère, soit la clé de contrôle, sera explicitée. Tous les chiffres de l'ISBN sont compris entre 0 et 9. Soit l'ISBN 978-0-387-69212-? du livre *Mathématiques et Technologie* de Christiane Rousseau et Yvan Saint-Aubin qui est une des sources de cet article. Pour remplacer le point d'interrogation par la clé de contrôle adéquate il faut calculer la somme des a_iu_i pour i de 1 à 12 où $a_i=3$ si i pair et $a_i=1$ si i impair. Nommons cette somme s. Alors, u_{10} est 0 si s est divisible par 10 $(0 \bmod 10)$. Sinon, u_{10} est 10 auquel on soustrait le reste de la division entière de s par 10. Dans l'exemple,

$$s = (1\times9) + (3\times7) + (1\times8) + (3\times0) + (1\times3) + (3\times8) + (1\times7) + (3\times6) + (1\times9) + (3\times2) + (1\times1) + (3\times2) \equiv 2 \bmod 10$$

Donc, la clé de contrôle est 10 – 2 = 8. L'ISBN complet est alors, 978-0-387-69212-8. Dans leur ouvrage, Christiane Rousseau et Yvan Saint-Aubin mentionnent l'ISBN à 10 chiffres et non à 13 chiffres. Le nombre de chiffres dans l'ISBN est passé de 10 à 13 en 2007, ce qui modifie légèrement le calcul de la clé.

On appelle donc l'ISBN un code détecteur, car si la dernière entrée ne coïncide pas avec celle calculée par la méthode expliquée précédemment on peut conclure qu'il y a une erreur. Cependant, on ne peut pas corriger cette erreur, car on ne peut pas savoir si c'est la clé ou l'une des 12 autres entrées du message reçu w qui a été altérée. Dans ce contexte, cette limitation n'est pas grave, car on veut seulement être capable de déterminer si un certain ISBN correspond vraiment à un document ou non. Dans le cas où un message important est transmis, on veut pouvoir corriger et interpréter le message tout de suite sans demander la retransmission de celui-ci. En particulier, les codes de Hamming et ceux de Reed-Solomon permettent d'identifier et de corriger l'erreur.

BÉATRICE HAJJAR, ÉTUDIANTE AU BACCALAURÉAT
EN MATHÉMATIQUES PURES ET APPLIQUÉES

LES PSEUDO-MATHÉMATIQUES

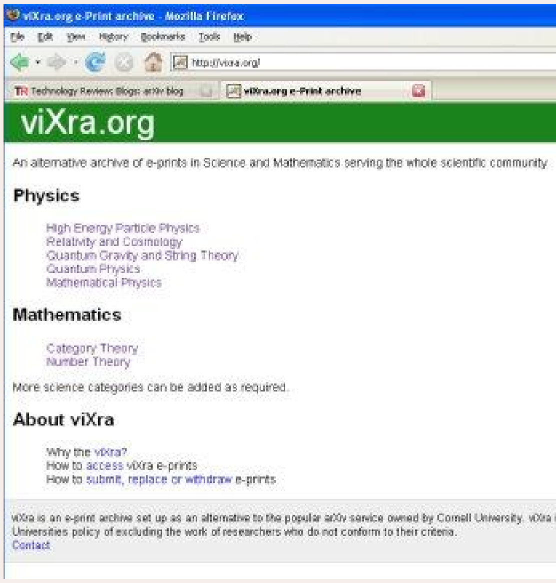
ET CEUX QUI LES FONT

C'est en physique que l'on rencontre la plus grande part des pseudo scientifiques[1], mais les mathématiques ont aussi leur lot de pseudo mathématiciens. Ils opérent en général en marge des institutions académiques, même si certains possèdent des diplômes universitaires[2]. Si certains rénovent de fond en comble les mathématiques, d'autres, plus modestes, se contentent de démontrer l'hypothèse de Riemann et de réaliser la quadrature du cercle.

Pour aller à leur rencontre et à celle de leurs découvertes étranges, il faut se rendre sur viXra, le double obscur et non-modéré d'arXiv, dont le service d'hégergement de PDF fait office de réseau de publication parallèle. D'ailleurs, la quantité d'articles qui s'y trouvent impressionne : plus de 36 000 articles sont répertoriés sur le site. On peut trouver de tout et surtout n'importe quoi, comme un document de 162 pages qui contient les solutions à tous les problèmes du prix du millénaire, des «spreadsheets» Excel qui démontrent le dernier théorème de Fermat, ou un article dont le titre, «la personnalité des nombres», doit être pris au pied de la lettre. Dans la section théorie des nombres, un article sur deux traite de l'hypothèse de Riemann, tantôt pour la démontrer, tantôt pour l'infirmer. Comme titres d'articles les plus surprenants, on pourrait mentionner l'équivoque «algèbre»[3], le mystérieux «le prochain infini est zéro», le bienveillant «gare aux arnaques», le morose «la fin des mathématiques», et enfin «pourquoi les mathématiques finies sont les plus fondamentales et la théorie quantique ultime sera basée sur les mathématiques finies». Le plus souvent les explications sont minimales, quelques lignes de calcul ou un dessin, lorsqu'elles ne sont pas complètement absentes. Si l'auteur développe davantage, c'est pour vanter son génie ou accuser les mathématiciens «ordinaires» de mauvaise foi, de méchanceté ou de jalousie à son égard.

Comment les reconnaître?

Le mathématicien John Baez a proposé en 1998 une liste de critères permettant de déterminer si on a affaire à un authentique scientifique ou à un *crackpot*. Parmi ceux-ci on retrouve «écrire des mots entiers en majuscules» , «nommer des théorèmes d'après soi-même», «faire allusion à des délais dans la recherche dus à un passage en asile psychiatrique» et «affirmer que sa théorie a d'abord été développé par une civilisation extraterreste».



ÉLOI MARTIN, ÉTUDIANT AU BACCALAURÉAT EN MATHÉMATIQUES PURES ET APPLIQUÉES

1. Aussi appelés en anglais *cranks*, *crackpots ou trisectors* (du problème classique de la trisection de l'angle).
2. De façon (plus ou moins) curieuse, un grand nombre d'entre eux sont ingénieurs.
3. Avec comme résumé : «cet article soulève des questions à propos de l'algèbre».

COMMENT GÉNÉRER DES NOMBRES (PSEUDO) ALÉATOIRES?

Dans le contexte de simulations par ordinateur, nous utilisons souvent des nombres aléatoires. Cependant, rares sont les gens qui n'ont pas déjà entendu que les ordinateurs ne peuvent PAS générer de nombres aléatoires. Cela semble contradictoire direz-vous ? La réalité est qu'ils ne peuvent créer que des nombres pseudoaléatoires. Cela soulève alors la question comment fonctionnent ces boites noires qui nous crachent des nombres ? Afin de mieux comprendre la situation, voici un exemple d'un algorithme qui génère des nombres pseudoaléatoires.

L'algorithme de Wichmann-Hill, proposé en 1982 par Brian Wichmann et David Hill, est relativement simple. Pour le comprendre, il faut savoir ce qu'est un générateur congruentiel linéaire (linear congruential generator, souvent abrégé **LCG**). Ces générateurs sont définis à l'aide de relations de récurrences de la forme $X_{n+1} = (aX_n+c) \bmod m$ qui définissent des suites de nombres entièrement connues dès qu'on a les paramètres et qu'on a choisi le premier nombre de la suite, X_0, appelé la graine ou le «seed» en anglais. L'algorithme de Wichmann-Hill utilise trois de ces LCG avec comme modulo **m** trois nombres premiers assez grands (respectivement 30269, 30307 et 30323). Pour ce qui est des paramètres ***a*** et ***c***, les créateurs ont choisi de ne pas prendre de ***c*** et d'utiliser comme multiplicateur ***a*** des racines primitives de ces nombres premiers (171, 172 et 170). Une racine primitive d'un premier ***p*** est un nombre qui a ***p-1*** puissances différentes modulo ***p*** (donc un ordre multiplicatif de ***p-1***). Ainsi, les trois générateurs ont une période de 30268, 30306 et 30322 puisqu'il faut multiplier le «seed» ce nombre de fois par le multiplicateur avant d'y revenir. Pour obtenir le nombre pseudoaléatoire, il suffira de diviser chaque nombre obtenu des trois générateurs par le nombre premier de leur modulo, les additionner ensemble et prendre la partie fractionnaire. Le résultat sera un nombre entre 0 et 1 et la prochaine itération de l'algorithme en donnera un autre, les nombres obtenus auront un comportement similaire à une loi uniforme sur [0,1]. Cependant, les nombres sont pseudoaléatoires et non aléatoires puisque si on connait l'état des générateurs à un certain moment, les prochains nombres peuvent être déterminés aisément. En fait comme les trois LCG sont indépendants, la période complète sera de 6.95 × 1012 ce qui est suffisamment grand pour qu'on ne se rende pas du tout compte que la suite de nombre se répètera un jour. Voici un bout de code Python illustrant l'algorithme et les 10 premiers nombres générés par celui-ci.

```python
r, s1, s2, s3 = 0, 100, 100, 100

def wichmannHill():
    global r, s1, s2, s3
    s1 = (171 * s1) % 30269
    s2 = (172 * s2) % 30307
    s3 = (170 * s3) % 30323

    r  = (s1/30269 + s2/30307 + s3/30323) % 1
```

```
0.6930906199656834
0.5253911237999249
0.14910212164520753
0.9526796411193339
0.8229855100670485
0.8003992983171554
0.9827082494536942
0.9718406372176753
0.928746025390614З
0.19793146562638286
```

Ici r est notre nombre «aléatoire» et ***s1, s2*** et ***s3*** sont nos générateurs congruentiels linéaires. On prend comme « seed » les trois valeurs initiales équivalentes à 100, mais habituellement on utilise l'horloge de l'ordinateur pour déterminer des valeurs initiales non-nulles moins prévisibles. Un fait intéressant à propos de l'algorithme est qu'on peut prouver par le théorème du reste chinois qu'il est en fait équivalent à un seul LCG avec comme multiplicateur ***a = 16 555 425 264 690*** et comme modulo ***m = 27 817 185 604 309***, cependant ces constantes sont beaucoup trop grandes pour être utilisées et il est beaucoup plus simple d'additionner trois LCG.

Enfin, l'algorithme de Wichmann-Hill n'en est qu'un parmi tant d'autres. Il est loin d'être le plus rapide, le plus efficace ou le plus sécuritaire, mais il reste intéressant. Parmi les autres, il y a le Mersenne Twister qui a une très grande période qui est un nombre premier de Mersenne (il est très utilisé et est notamment le générateur de nombre aléatoire de Python et de R). Toutes les années, de nouveaux algorithmes sont créés et les anciens sont souvent révisés alors c'est un monde complet à découvrir.

MATHIEU PINEAULT, ÉTUDIANT AU BACCALAURÉAT EN MATHÉMATIQUES PURES ET APPLIQUÉES

AUX GRANDS MAUX LES GRANDS REMÈDES

D'une manière très éloquente, la pandémie actuelle a mis en lumière les lacunes de notre système de santé. Nous pouvons notamment penser à la crise des centres d'hébergement de soins de longue durée (CHSLD), au manque de travailleurs dans le réseau de la santé et aux hôpitaux débordés. Or, un autre élément relatif plus ou moins abordé dans la société a fait plusieurs fois la manchette ces dernières années. Dans le rapport de la commission Hoskins, on montre qu'en 2019, près de 7,5 millions de Canadiens, soit environ 20% de la population, n'avaient pas d'assurance médicaments ou ne possédaient pas une assurance suffisante pour répondre à leurs besoins. Pour combler cette disparité, le gouvernement fédéral voudrait instaurer un régime d'assurance médicaments universel public et à payeur unique. Toutefois, «cette solution n'est [peut-être] pas la plus efficace», déplore l'Institut canadien des actuaires (ICA) qui suggère une alternative dans sa publication de février 2021 «*Régime d'assurance médicaments : Y a-t-il une pilule pour ça?*»

Au lieu de repartir à zéro, l'ICA propose de bâtir un plan sur ce qui existe déjà, c'est-à-dire les régimes privés et publics actuels, pour en élargir la couverture à tous les Canadiens. Tout d'abord, un organisme de surveillance coopératif, formé de représentants des gouvernements fédéral, provinciaux et territoriaux ainsi que de l'industrie de l'assurance et de spécialistes concernés, devra être mis sur pied pour établir une liste nationale des médicaments assurés et pour négocier les prix des médicaments au nom de tous les assureurs du Canada. Ainsi, les régimes publics et les régimes privés devront couvrir au minimum tous les médicaments figurant dans la liste nationale des médicaments. De plus, le coût assumé par les patients sous forme de franchise et de coassurance sera limité à un montant abordable. Quant au rôle du gouvernement fédéral, ce denier assumera la part du coût des médicaments des assurés des régimes publics et privés qui excéderait une limite prédéterminée. Celui-ci prendra aussi en charge le coût de certains médicaments très coûteux inscrits sur la liste pour les maladies rares. Cette mutualisation des coûts au sommet permettrait d'absorber le risque et de partager les réclamations coûteuses entre les différents organismes.

Cela dit, quels avantages tirerait la Belle Province, qui a déjà la Régie de l'assurance maladie du Québec (RAMQ), si elle devait joindre ce nouveau programme? Présentement, le régime public québécois inclut plus de 8 000 médicaments assurés dans sa liste, mais certains régimes privés en couvrent davantage. Pour un citoyen québécois, le coût des médicaments absents de la liste provinciale actuelle, mais présents sur la liste nationale sera couvert. D'ailleurs, malgré les efforts du Québec pour maîtriser le coût de son programme universel, il a été impossible de limiter la hausse des coûts à l'inflation générale. En fait, ce cas s'applique également pour la majorité des régimes d'assurance médicaments publics et privés au cours de la même période. Dans sa publication, l'ICA dénote le fait qu'entre 1997 et 2020, les assurés de la RAMQ ont vu passer leurs primes annuelles de 175$ par adulte (l'équivalent de 265$ en 2020) à 648$ par adulte, une hausse de 145% par rapport à l'inflation. Par conséquent, une aide fédérale, un partage des risques et une négociation des prix des médicaments à grande échelle permettraient de réduire la volatilité des coûts et d'allouer des budgets plus stables aux provinces.

En conclusion, d'un point de vue actuariel, l'ICA considère qu'une couverture des médicaments sur ordonnance pour tous les Canadien.ne.s favoriserait non seulement une meilleure espérance de vie, mais aussi une productivité accrue des travailleurs sur le marché ce qui entrainerait une croissance économique favorable. De plus, cette initiative permettrait de réduire le recours à certains éléments plus coûteux de nos ressources limitées en soins de santé, notamment les hôpitaux.

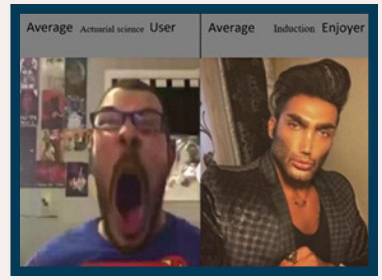
Après les coûts hospitaliers et avant les services de médecins, les médicaments sur ordonnance représentent la deuxième plus importante dépense dans le domaine de la santé au Canada avec 34 milliards de dollars en 2018

Environ 21 millions de Canadiens sont couverts par des régimes privés qui exigent généralement des primes et des quotes-part

La part fédérale dans le financement de l'assurance maladie publique des provinces et des territoires est passé de 50% à moins de 25%

SIMON LUANGXAY, ÉTUDIANT AU BACCALAURÉAT EN ACTUARIAT

| GALERIE



| JEU MATHÉMATIQUE

Pour les amateurs de sudokus, voici un Kendoku (aussi appelé Calcudoku).

Remplissez la grille suivante avec les chiffres de 1 à 6 de sorte que chaque ligne et chaque colonne contienne chacun des chiffres une seule fois. De plus, il faut que chaque groupe entouré de lignes foncées donne le nombre dans le coin supérieur gauche en utilisant l'opération arithmétique spécifiée (addition, soustraction, multiplication ou division).

7 +		3 ÷	4 ÷		11 +
4 ÷			6 ÷		
14 +				2 ÷	
5 +		20 ×		5 -	
12 ×			7 +		24 ×
	1 -		5 +		

semaine du bien-être

5 – 9 avril 2021

Visitez la page Facebook de l'événement pour tous les détails!

FAECUM.QC.CA

FAÉCUM