

HORS-SÉRIE N° 103 : NOMBRES

L'énigme de la capsule temporelle est résolue !

Bernard Fabrot, un programmeur indépendant belge, est venu à bout d'une énigme posée il y a vingt ans par l'un des créateurs du système RSA. La solution n'était attendue qu'en 2035...

Les nombres sont au cœur de nombreuses énigmes, dont plusieurs étaient proposées dans le *Hors-Série* n° 103 : «L'ordre caché des nombres». L'une d'elles vient d'être résolue par le Belge Bernard Fabrot, programmeur indépendant.

En 1999, à l'occasion du 35^e anniversaire du Laboratoire d'informatique du MIT, le cryptologue américain Ronald Rivest (l'un des trois inventeurs de l'algorithme de cryptographie à clé publique RSA) enferme dans une «capsule temporelle» conçue par l'architecte Frank Gehry plusieurs objets offerts par les pionniers du numérique comme Bill Gates, Bob Metcalfe, Tim Berners-Lee... et promet le contenu à celui qui résoudra le défi suivant, noté LCS35 :

Calculer $w = 2^{2^t} \pmod n$, pour $t = 79685186856218$ et n un entier donné de 616 chiffres décimaux, produit de deux grands nombres premiers (qui ne sont pas connus). Trouver la valeur de w sans connaître la factorisation de n oblige à effectuer quelque 80000 milliards d'opérations itérées de mise au carré modul n en commençant par 2. À la fin, on peut traduire le résultat obtenu, w , en une phrase qui est le Sésame de la capsule.

Le problème a été conçu de façon à empêcher tout calcul parallèle. C'est un exemple de

«fonctions à retard vérifiable» (notées VDF pour *Verifiable Delay Functions*), aujourd'hui étudiées pour sécuriser les blockchains, sur lesquelles reposent, par exemple, le bitcoin ou Ethereum. C'est un des thèmes de recherche de Cryptophage, un groupe d'experts en cryptographie dirigé par Simon Peffers, d'Intel, qui planchait également sur le problème de Ronald Rivest. Ils ont été coiffés sur le fil par Bernard Fabrot.

Celui-ci a découvert par accident l'énigme en 2015. Il en est venu à bout à l'aide de GNUMP, une bibliothèque logicielle de calculs sur des nombres entiers, qui a accaparé une partie de son ordinateur personnel (plus précisément, un cœur du microprocesseur) 24 heures sur 24 et sept jours sur sept, vacances exceptées, pendant trois ans et demi. Il devance ainsi de quinze ans les prédictions de Ronald Rivest, fondées sur la loi de Moore.

Surprise, lorsqu'il envoie son résultat, le laboratoire de Ronald Rivest n'existe plus : il est intégré dans une entité plus grande (le CSAIL) dont la directrice n'a jamais entendu parler du problème. Tout s'est bien terminé, par une cérémonie le 15 mai 2019 lors de laquelle la capsule temporelle a été ouverte. ■

LE COMMUNIQUÉ DU CSAIL : [HTTP://BIT.LY/CSAIL-LCS35](http://bit.ly/CSAIL-LCS35)

Le contenu de la capsule temporelle est dévoilé devant notamment celui qui en a eu l'idée, Ronald Rivest (à droite), et celui qui a réussi à l'ouvrir, Bernard Fabrot (à sa droite).



Une mémoire fondée sur l'aléa

La mémoire de travail, l'une de celles décrites dans le *Hors-Série* n° 102 : «Les mutations de notre mémoire», permet notamment de garder à l'esprit le nécessaire à l'accomplissement d'une tâche. Comment fonctionne-t-elle ? Flora Bouchacourt et Timothy Buschman, de l'université de Princeton, aux États-Unis, proposent un nouveau modèle plus en accord avec les observations que les précédents, mettant en jeu des connexions aléatoires récurrentes selon deux «couches» neuronales, l'une étant liée aux perceptions sensorielles afin de maintenir l'afflux d'informations.

F. BOUCHACOURT
ET T. BUSCHMAN, *NEURON*,
PRÉPUBLICATION EN LIGNE, 2019

La nature, bonne pour... la nature

Les bains de nature sont bons pour la santé, les articles du *Hors-Série* n° 101 : «La révolution végétale» en attestent. Ils sont aussi bons pour la planète ! C'est le sens des résultats obtenus par Victor Cazalis (CEFE) et Anne-Caroline Prévot (CESCO). À partir de trois indicateurs (le score des candidats écologistes à diverses élections, le soutien aux associations environnementales et la participation à un programme de sciences participatives), ils ont montré que les Français ont des comportements d'autant plus écologiques qu'ils habitent dans un parc naturel (national ou régional), ou même simplement à proximité. On ne peut donc qu'encourager ces aires protégées, qui préservent le lien entre humains et nature, à poursuivre leurs actions. Et souhaiter voir le monde entier devenir parc naturel !

V. CAZALIS ET A.-C. PRÉVOT,
BIOLOGICAL CONSERVATION,
PRÉPUBLICATION EN LIGNE, 2019

Pastèque et musique nigériane

L'été est là, ses pics de chaleur et ses envies de rafraîchissement. Quoi de mieux qu'une pastèque? Oui, certes, mais comment la choisir? En habituant votre oreille aux sons des tambours nigériens. C'est l'étonnante découverte du chercheur et chanteur nigérien Stephen Onwubiko qui a été présentée lors du 177^e congrès de la Société américaine d'acoustique, à Louisville, dans le Kentucky, aux États-Unis, du 13 au 17 mai 2019. Une nouvelle vertu de la musique à ajouter à celles décrites dans le *Hors-Série* n° 100: «Good vibrations»!

Lorsque vous hésitez face à un choix de pastèques, vous tapotez les fruits en espérant repérer le plus mûr. Stephen Onwubiko a étudié la perception de ces sons chez des vendeurs et des consommateurs. Puis, avec la physicienne Tracianne Nielsen, de l'université Brigham Young, dans l'Utah, et la musicologue Andrea Calilhanna, de l'université de Sydney, en Australie, ils ont ensuite analysé ces sons et les ont comparés à ceux des igba, des tambours traditionnels du pays. Les points communs sont nombreux et, en particulier, les sons produits par des pastèques mûres ou non se retrouvent dans le répertoire musical.

Selon les chercheurs, les ingrédients de la musique traditionnelle nigérienne (la hauteur, les rythmes, les décalages, les syncopes...) constitueraient au final l'entraînement parfait pour identifier les pastèques prêtes à être consommées. Une astuce à utiliser rapidement: les sons produits par une pastèque sont de plus en plus clairs à mesure qu'elle gagne en maturité. L'été s'annonce bien, avec des concerts sur les étals des marchés! ■

S. ONWUBIKO ET AL., *THE JOURNAL OF THE ACOUSTICAL SOCIETY OF AMERICA*, VOL. 145, ART. 1708, 2019

Le World Wood Wide Web

Champignons et bactéries relient les arbres et tissent un Wood Wide Web. La cartographie mondiale de ces symbioses révèle leur rôle clé dans la régulation du climat.



Les arbres des forêts tropicales et les microorganismes associés sont moins bénéfiques pour le climat que leurs homologues des régions tempérées et froides.

Sans les champignons, les forêts n'existeraient pas, le *Hors-Série* n° 101: «La révolution végétale» le prouvait. De fait, les arbres profitent des bienfaits que leur procurent les champignons et les bactéries avec lesquels ils sont en étroite association. Par exemple, avec les très nombreuses ramifications de leurs filaments (les hyphes), les champignons explorent un volume de sol beaucoup plus important que les seules racines de l'arbre et transfèrent à ce dernier eau et sels minéraux. Ces hyphes permettraient également aux arbres de communiquer et certains n'hésitent pas à parler de Wood Wide Web. Une équipe internationale, emmenée par Brian Steidinger, de l'université Stanford, aux États-Unis, a entrepris d'étudier à l'échelle mondiale les relations symbiotiques entre les arbres et leurs microorganismes, champignons mycorhiziens et bactéries fixatrices d'azote.

À partir des données de la *Global Forest Initiative*, 31 millions d'arbres de 28 000 espèces, répartis dans 70 pays de tous les continents (sauf Antarctique) ont été pris en compte. On apprend que le type de mycorhize dépend du climat. Les ectomycorhizes (les hyphes entourent simplement les racines de l'arbre) sont notablement plus abondantes dans les régions tempérées et froides que les endomycorhizes (les hyphes pénètrent à l'intérieur des racines de l'arbre). Or avec les premières (60% des arbres mondiaux pour seulement 2% des espèces!), la séquestration du carbone dans le sol est plus importante, grâce à des composés secondaires inhibant la dégradation de la matière organique.

Avec le réchauffement du climat, les auteurs de l'étude prévoient une baisse de 10% des champignons ectomycorhiziens et des arbres qui leur sont associés. La conséquence? Une nouvelle augmentation du carbone atmosphérique... Les projets de reboisement, notamment celui du Programme des Nations unies pour l'environnement, doivent en tenir compte. ■

B. S. STEIDINGER ET AL., *NATURE*, VOL. 569, PP. 404-408, 2019

HORS-SÉRIE N° 102 : MÉMOIRE

Alzheimer : la maladie à deux prions

Les deux protéines caractéristiques de la maladie d'Alzheimer – les protéines bêta amyloïdes et les protéines tau anormales – agiraient bien comme des prions, le type d'agents infectieux en cause dans la maladie de la vache folle.

Selon l'Organisation mondiale de la santé, 135 millions de personnes seront touchées par la maladie d'Alzheimer d'ici à 2050, rappelait le *Hors-Série* n° 102 : «Les mutations de notre mémoire». C'est dire que la course contre la montre pour comprendre et vaincre cette maladie est lancée ! Une avancée importante vient d'être accomplie par l'équipe de Stanley Prusiner, de l'université de Californie, à San Francisco, aux États-Unis : les protéines qui déclenchent cette maladie agissent comme des prions.

Les deux protéines en question sont les peptides bêta amyloïdes qui s'accumulent en plaques (dites amyloïdes) en dehors des neurones et les protéines tau anormales (elles sont hyperphosphorylées). Ces dernières déstabilisent les microtubules, les rails moléculaires le long desquels circulent divers messagers dans la cellule.

Les prions, dont la découverte en 1982 a valu à Stanley Prusiner le prix Nobel de médecine en 1992, sont des agents infectieux d'un genre nouveau : ce sont des protéines mal repliées qui transmettent leur anomalie à d'autres en cours de formation. Ce type de dysfonctionnement est impliqué notamment dans

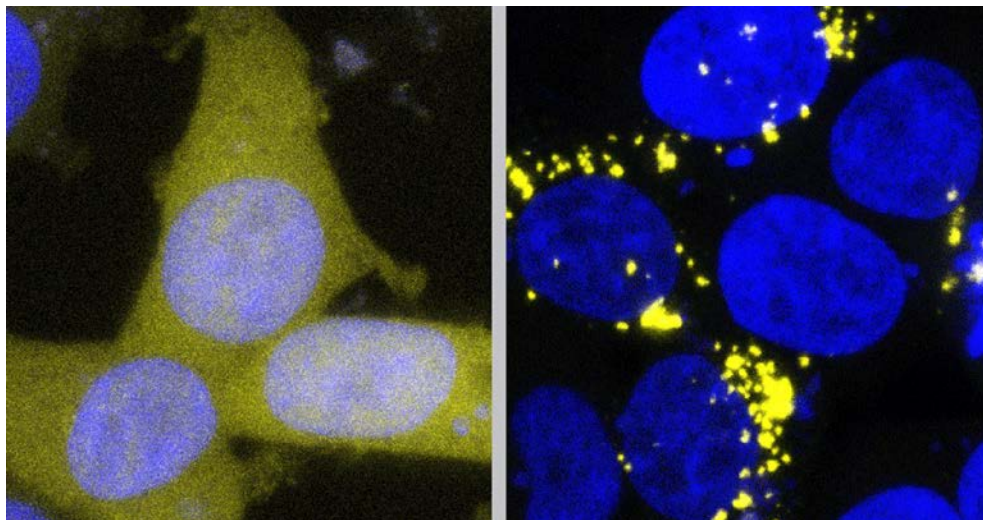
l'encéphalopathie spongiforme bovine, la maladie de Creutzfeldt-Jakob... Comment sont reliés les prions à la maladie d'Alzheimer ?

Dès 2012, Stanley Prusiner avait montré que la protéine bêta amyloïde se diffuse dans le cerveau, un premier indice plaçant pour un comportement de prion. Après d'autres travaux allant dans ce sens, les biologistes ont cette fois mis au point de nouveaux outils permettant de mesurer les quantités de protéines circulantes : ils les ont utilisés pour révéler l'activité de type prion des protéines bêta amyloïdes et tau anormales dans le tissu cérébral de 75 patients atteints d'Alzheimer d'âges divers (après leur mort) qu'ils ont comparée avec celle d'individus souffrant d'autres formes de démence (quelque 25 cas).

La maladie d'Alzheimer serait donc une pathologie à double prion. Selon les auteurs, de nouvelles voies menant à des tests de dépistage et des médicaments d'un type inédit sont désormais ouvertes... même si on ignore encore aujourd'hui comment éliminer les prions ! ■

A. AOYAGI ET AL., *SCIENCE TRANSLATIONAL MEDICINE*, VOL. 11, ISSUE 490, EAAT8462, 2019

La protéine bêta amyloïde (en jaune) normale est présente de façon diffuse dans les neurones (à gauche). Dans la maladie d'Alzheimer, elle s'agrège (à droite) en petits congloمرats.



Multiplication express

Pour multiplier deux nombres à 3 chiffres en suivant la méthode apprise à l'école, $3 \times 3 = 9$ multiplications élémentaires sont nécessaires, le *Hors-Série* n° 103 : «L'ordre caché des nombres» en parlait. Et avec des nombres à n chiffres, n^2 multiplications sont requises... c'est long, surtout quand n est très grand ! Joris van der Hoeven, de l'École polytechnique, et David Harvey, de l'université de Nouvelle-Galles du Sud, en Australie, ont mis au point un algorithme beaucoup plus rapide. Le nombre de multiplications intermédiaires est désormais en $n \log n$, et c'est probablement le meilleur résultat possible. En théorie, on peut donc multiplier deux nombres à 100 chiffres en seulement 200 opérations au lieu des 10 000. Problème, l'algorithme ne fonctionne pour l'instant que pour de très grands nombres. Les mathématiciens espèrent néanmoins identifier des variantes de l'algorithme pouvant s'appliquer à des nombres plus petits.

D. HARVEY ET J. VAN DER HOEVEN, 12 AVRIL 2019 : [HTTPS://HAL.ARCHIVES-OUVERTES.FR/HAL-02070778](https://hal.archives-ouvertes.fr/hal-02070778)

Dépression et musique triste

La musique est bonne pour la santé, le *Hors-Série* n° 100 : «Good vibrations» en apportait plusieurs preuves. Pourtant, on peut se demander pourquoi les personnes dépressives préfèrent-elles les musiques tristes, celles-ci ne semblant pas améliorer leur état ? Une étude de Jonathan Rottenberg, de l'université de Floride du Sud, et de ses collègues, apporte une réponse inattendue. Des travaux précédents avaient proposé que la motivation de ce comportement était d'augmenter l'état dépressif, ou au moins le maintenir. Selon les chercheurs, c'est en fait plutôt un effet calmant et relaxant qui est recherché.

S. YOON ET AL., *EMOTION*, PRÉPUBLICATION EN LIGNE, 2019

ABONNEZ-VOUS À POUR LA SCIENCE

2 FORMULES
AU CHOIX

	FORMULE PAPIER + HORS-SÉRIE	FORMULE INTÉGRALE
Le magazine papier (12 numéros par an)	✓	✓
Le hors-série papier (4 numéros par an)	✓	✓
L'accès en ligne illimité à pourlascience.fr		✓
L'édition numérique du magazine (12 numéros par an)		✓
L'édition numérique du hors-série (4 numéros par an)		✓
L'accès aux archives numériques depuis 1996		✓
VOTRE TARIF D'ABONNEMENT	79€ Au lieu de 114,40€	99€ Au lieu de 174,40€

31 %
de réduction *

43 %
de réduction *

BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à :

Pour la Science – Service abonnements – 19 rue de l'Industrie – BP 90053 – 67402 Illkirch Cedex – email: pourlascience@abopress.fr

PAG19STDDOS



**OUI, je m'abonne
pour 1 an à**
POUR LA SCIENCE

1 / Je choisis ma formule (merci de cocher)

☐ FORMULE PAPIER + HORS SÉRIE

- 12 n° du magazine papier
- 4 Hors-série papier

79€
Au lieu de 114,40€
PTA79E

☐ FORMULE INTÉGRALE

- 12 n° du magazine papier
- 4 Hors-série papier
- Accès illimité aux contenus en ligne

99€
Au lieu de 174,40€
ITA99E

2 / J'indique mes coordonnées

☐ M. ☐ Mme

Nom : Prénom :

Adresse :

Code postal [] [] [] [] [] [] Ville :

Téléphone [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] []

Email : (indispensable pour la formule intégrale)

.....@.....

J'accepte de recevoir les offres de Pour la Science

☐ OUI ☐ NON

3 / Je choisis mon mode de règlement

☐ Par chèque à l'ordre de Pour la Science

☐ Carte bancaire

N° [] [] [] [] [] [] [] [] [] [] [] [] [] [] [] []

Date d'expiration [] [] [] [] Clé (Les 3 chiffres au dos de votre CB) [] [] []

Signature obligatoire :

* Réduction par rapport au prix de vente en kiosque et l'accès aux archives numériques. Durée d'abonnement: 1 an. Délai de livraison: dans le mois suivant l'enregistrement de votre règlement. Offre valable jusqu'au 31/12/2019 en France métropolitaine uniquement. Pour un abonnement à l'étranger, merci de consulter notre site <https://boutique.pourlascience.fr>. Photos non contractuelles.

Les informations que nous collectons dans ce bulletin d'abonnement nous aident à personnaliser et à améliorer les services que nous vous proposons. Nous les utiliserons pour gérer votre accès à l'intégralité de nos services, traiter vos commandes et paiements, et vous faire part notamment par newsletters de nos offres commerciales moyennant le respect de vos choix en la matière. Le responsable du traitement est la société Pour la Science. Vos données personnelles ne seront pas conservées au-delà de la durée nécessaire à la finalité de leur traitement. Pour la Science ne commercialise ni ne loue vos données à caractère personnel à des tiers. Les données collectées sont exclusivement destinées à Pour la Science. Nous vous invitons à prendre connaissance de notre charte de protection des données personnelles à l'adresse suivante: <https://rebrand.ly/charte-donnees-pls>. Conformément à la réglementation applicable (et notamment au Règlement 2016/679/UE dit « RGPD ») vous disposez des droits d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation de vos données personnelles. Pour exercer ces droits (ou nous poser toute question concernant le traitement de vos données personnelles), vous pouvez nous contacter par courriel à l'adresse protection-donnees@pourlascience.fr.