

La catastrophe d'octobre 1979 est survenue au troisième jour de forte crue du Var. La charge sédimentaire en suspension a peut-être suffi à donner à l'eau douce chargée une densité supérieure à celle de l'eau de mer : le cours du fleuve se serait alors poursuivi au fond de la mer et aurait érodé les flancs instables du canyon du Var.

P. COUPRIE, Paris

Réponse de Philippe Heinrich

Je ne suis pas opposé à la thèse qu'un tsunami engendré au large aurait précédé l'effondrement de la digue et des sédiments sous-jacents, et de ce fait serait à l'origine de l'effondrement. Toutefois, elle ne fait pas l'unanimité, précisément en raison des contradictions entre les témoignages sur la chronologie des observations des vagues en différents points de la côte.

Les simulations numériques révèlent que l'effondrement de dix millions de mètres cubes de sédiments situés à proximité de la surface de l'eau engendre une vague de quelques mètres de hauteur localement, suffisante pour inonder les terrains situés en face de l'aéroport. Il n'a jamais été conclu que cet effondrement est à l'origine d'un tsunami. Bien au contraire, les simulations ont montré aussi que les vagues engendrées par cet effondrement n'expliquent pas le tsunami observé dans la Baie des Anges. Les modélisations que nous avons effectuées simulent des phénomènes hydrodynamiques, tels le déplacement d'un fluide par le mouvement d'une masse et la propagation d'ondes à la surface de l'eau. Elles ne permettent pas de conclure sur l'antériorité ou non de l'effondrement de la digue, ni sur la cause de cet effondrement.

L'origine de la vie

Pourquoi la vie a-t-elle plus de chances de venir d'une autre planète du Système solaire que de la Terre, alors qu'elles ont toutes à peu près le même âge (voir *Origine extraterrestre ?*, par C.-A. Roten, *Pour la Science*, juillet 1999)? Si elle vient d'un autre système planétaire, c'est un autre problème...

Frédéric MALHER, Paris

Réponse de C.-A. Roten

L'émergence de la vie est associée à l'existence d'une croûte planétaire solide. En son sein ou dans un océan, des molécules peuvent s'auto-organiser pour permettre l'apparition d'une première cellule. Tout corps orbitant autour du Soleil s'est formé il y a 4,6 milliards d'années. Suite au bombardement météoritique intense de l'ac-

création et à la chaleur émise par la fission des atomes radioactifs, les constituants de Mars et de la Terre se sont séparés pour former un noyau et un manteau. Par la suite, seule la chaleur émise par la fission nucléaire était suffisante pour empêcher la solidification d'une croûte planétaire. Comme Mars et la Terre ont une concentration d'atomes radioactifs similaire, Mars, plus petite, s'est refroidie plus rapidement car le rapport de sa surface à son volume est plus important que celui de notre planète. Mars, dont la surface s'est solidifiée avant celle de la Terre, a donc pu abriter les plus anciennes formes de vie du Système solaire.

Ginkgo costaud

Le *Ginkgo biloba* résiste à de nombreuses agressions (voir *La résistance des ginkgos*, *Pour la Science*, mai 1999) : il aurait même survécu à l'explosion atomique d'Hiroshima. Toutefois, ce n'est qu'à Kyoto que j'ai vu beaucoup de ginkgos le long des avenues. À Paris, malheureusement, je ne connais que celui du Jardin des Plantes.

Claude CARDOT, Gif sur Yvette

Réponse de T. T. Nguyen Tu et H. Bocherens

À Hiroshima, un *Ginkgo biloba* a effectivement survécu à la bombe atomique : ses feuilles ont repoussé au printemps suivant l'explosion bien que son appareil végétatif ait entièrement brûlé. L'implantation des ginkgos dans les villes est de plus en plus importante, non seulement au Japon, mais aussi en Europe. De nombreux boulevards et parcs de Tokyo sont plantés de ginkgos. À Paris, son implantation est plus récente : tous les marronniers bordant les avenues n'ont pas été remplacés par des ginkgos! Mais dès que des arbres sont à planter le choix est le plus souvent porté sur le ginkgo, par exemple au Musée de sculpture en plein air, sur le quai Saint Bernard.

Lettre codée

Dans l'article *Paiements sur l'Internet* (voir *Pour la Science*, juin 1999), Octavian Ureche et Réjean Plamondon écrivent : «Ce système est relativement sûr : en Europe, le protocole SSL chiffre les données avec des clés de 40 bits. Autrement dit, pour percer le code de chiffrement, il faudrait trouver les facteurs premiers d'un nombre de 40 bits (ou 10 chiffres), ce qui prendrait des jours à un ordinateur de bureau.» Je pense qu'il y a ici une confusion : la clé de 40 bits utilisée

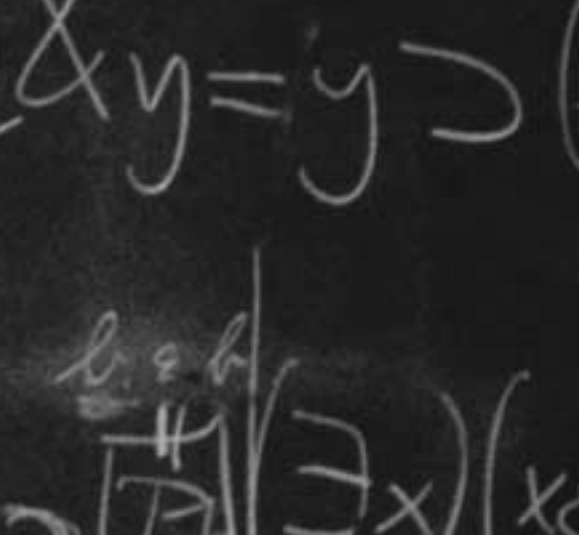
est la clé d'encryptage symétrique (plus précisément, la partie secrète de cette clé, l'algorithme utilisé (RC4) étant de type «stream cipher», chaque message a une clé différente). Cette clé est encodée au moyen d'un algorithme à clé publique, utilisant une clé beaucoup plus grande. La factorisation d'un nombre de 40 bits (12 chiffres) prend moins d'une seconde...

Jacques WILLEKENS, Bruxelles

Réponse d'Octavian Ureche et Réjean Plamondon

Le protocole SSL implique plusieurs phases. Une première phase consiste en l'établissement du lien encrypté de communication entre le client et le serveur. Cette phase est elle-même formée de deux étapes : l'authentification du serveur et l'authentification (optionnelle) du client. La deuxième phase consiste en l'envoi proprement dit des données. Si la première phase utilise effectivement un chiffre asymétrique, notamment le chiffre RSA, la deuxième phase utilise un chiffre symétrique. Lors de la première étape de la première phase, en répondant à la demande du client, le serveur envoie son certificat et ses préférences d'encryptage (le chiffre à utiliser, etc.). Le client crée une clé de session (chaque session, et non pas chaque message lors d'une même session, ayant une clé différente) et l'envoie au serveur, encryptée avec la clé publique de ce dernier. Le serveur décrypte la clé de session et s'identifie en retournant un message authentifié avec la clé de session. Toutes les données seront par la suite encryptées et authentifiées avec cette clé de session. La clé de session utilisée par un algorithme d'encryptage symétrique tel que RC4 a une longueur de quelques dizaines de bits, 40 jusqu'à tout récemment, 128 depuis peu de temps. Même s'il n'est pas trop difficile de craquer des clés très courtes, la cryptanalyse n'est pas à la portée de tout le monde. Toutefois, ceci est en train de changer avec la puissance croissante des ordinateurs personnels accessibles à des prix dérisoires. C'est pour de telles raisons que de plus en plus de gouvernements allègent leurs politiques en matière de cryptographie pour passer à des clés plus longues, donc plus sûres.

Écrivez à *Pour la Science* vos réactions, vos commentaires et vos réflexions sur l'actualité scientifique et vos relations avec la science. L'adresse de *Pour la Science* sur Internet est : tribune@pouirlascience.fr. D'autres contributions de lecteurs sont sur le site Web à <http://www.pouirlascience.com>.



Gödel et les limites de la logique

JOHN DAWSON

Le mathématicien Kurt Gödel a consacré ses travaux à la rationalité, alors que sa vie privée en était parfois dépourvue.

Le personnage qui est représenté sur la photographie ci-dessus n'est pas connu du grand public. Pourtant, ses théorèmes d'incomplétude et ses autres résultats de mathématiques ou de logique ont ébranlé les mathématiques et l'informatique. Toute sa vie, il rechercha la rationalité, mais dut lutter contre une profonde fragilité mentale.

Gödel a démontré que les méthodes mathématiques utilisées depuis Euclide ne peuvent révéler toutes les propriétés de l'ensemble des nombres entiers naturels. Sa découverte, qui bouleversa les mathématiques créées au xx^e siècle, a relancé la recherche de nouvelles voies d'étude et provoqué un débat philosophique sur la nature de la vérité. Les techniques inventées par Gödel, qui sont applicables aux algorithmes de calcul, ont également posé les fondations de l'informatique moderne.

Gödel naît le 28 avril 1906 à Brno, à 180 kilomètres au Sud-Est de Prague, en République tchèque. Il est le cadet des deux enfants de Rudolf et Marianne Gödel, des Allemands expatriés dont les familles travaillaient pour l'industrie textile locale. La famille ne comptait pas d'intellectuels, et son père n'avait reçu qu'une formation en techniques commerciales. Toutefois, ce dernier était ambitieux et travailleur : il sera progressivement directeur, puis actionnaire d'une importante usine de textile de Brno. Suffisamment enrichi, Rudolf Gödel acquiert une maison dans un quartier chic et envoie ses fils dans des écoles privées de langue allemande, où tous deux font de brillantes études.

De toute sa scolarité primaire et secondaire, le jeune Kurt n'a qu'une seule fois une note inférieure au maximum – en mathématiques ! Pourtant, ses talents restent insoupçonnés, car, malgré son insatiable curiosité (il est surnommé Monsieur Pourquoi), il est introverti, sensible et

plutôt maladif. Vers l'âge de huit ans, il contracte un rhumatisme articulaire aigu qui, bien que sans séquelles physiques, l'éloigne de l'école assez longtemps. Cette maladie est probablement l'une des causes de son hypochondrie.

L'INTROVERTI

En 1924, diplômé du lycée technique de Brno, Gödel quitte son pays natal pour l'Université de Vienne, où son frère a commencé ses études de médecine quatre ans plus tôt. Après la Première Guerre mondiale et la chute de l'empire austro-hongrois, Vienne est en ruine,

mais le prestige de l'Université est intact. Ainsi, malgré les privations matérielles, la Vienne de l'entre-deux-guerres est un centre scientifique littéraire et philosophique très actif.

Initialement inscrit en physique, Gödel s'oriente vers les mathématiques dès qu'il a suivi les cours de Phillip Furtwängler et de Hans Hahn (1879-1934). Il est vite remarqué : deux ans seulement après son arrivée, il est invité dans le groupe de travail fondé en 1924 par Hahn et par le philosophe néo-positiviste Moritz Schlick (1882-1936). Ce groupe, qui deviendra le Cercle de Vienne, est inspiré des écrits d'Ernst Mach (1838-1916), rationaliste pour qui seules la logique et l'observation empirique ont une valeur explicative ; la métaphysique est écartée.

Grâce au Cercle, Gödel rencontre des savants tels que le philosophe des sciences Rudolf Carnap (1891-1970) ou le mathématicien Karl Menger (1902-1985). Il se familiarise avec la logique mathématique et la philosophie, et, en particulier, avec les écrits de Ludwig Wittgenstein (1889-1951), dont la réflexion sur l'aptitude du langage à parler de lui-même a peut-être poussé Gödel à explorer les problèmes équivalents en mathématiques.

Avec certains membres du Cercle, dont Carnap, Hahn et le physicien Hans Thirring, il s'intéresse également aux phénomènes parapsychologiques. Des années plus tard, il confiera à son ami économiste Oskar Morgenstern (1902-1977) que, dans un futur lointain, on s'étonnera que les scientifiques du xx^e siècle aient découvert les particules physiques élémentaires, sans même envisager la possibilité de facteurs psychiques élémentaires.

Cependant, Gödel ne partage pas la vision philosophique positiviste du Cercle. Il est platonicien : en dehors des objets, un monde de concepts existe, accessible



1. LES DEUX FRÈRES GÖDEL, Kurt (à droite) et Rudolf étaient très proches ; ils se sont peu à peu éloignés à l'âge adulte. Ce cliché de studio date de 1908.

par l'intuition. Ainsi, toute proposition a une « valeur de vérité » (être vraie ou être fausse), que cette valeur ait été établie ou non par les mathématiques ou par un moyen expérimental. Il admettra ultérieurement que cette philosophie a facilité ses intuitions mathématiques.

Observateur attentif et brillant, Gödel s'exprime rarement lors des discussions du Cercle, sauf lorsqu'elles concernent les mathématiques. Timide et solitaire, il a peu d'amis intimes (cependant, il apprécie la compagnie des femmes, qui le trouvent séduisant). Après 1928, il délaisse peu à peu le groupe et s'investit dans un séminaire de mathématiques organisé par Menger. Gödel participe à la publication annuelle des actes ; il publiera ainsi une dizaine d'articles.

UN GÉNIE RÉSERVÉ

C'est l'époque à laquelle Gödel acquiert une réputation internationale en logique mathématique, notamment grâce à deux articles : sa thèse, soutenue à l'Université de Vienne en 1929 et publiée l'année suivante, et son traité *Sur les propositions formellement indécidables des Principia Mathematica et des systèmes apparentés*, publié en allemand en 1931 et présenté comme thèse d'habilitation à l'enseignement en 1932. Dans les *Principia Mathematica* de Bertrand Russell (1872-1970) et d'Alfred Whitehead (1861-1947), les auteurs proposent la logique comme fondement des mathématiques. Ils résolvent un problème posé en 1928, par David Hilbert (1862-1943) et par Wilhelm Ackermann (1896-1962) dans leurs *Fondements de la Logique théorique* : Hilbert et Ackermann y énoncent des règles de manipulation d'expressions logiques composées de connecteurs (et, ou...), de quantificateurs (pour tout, il existe...), et de variables (nombres, propositions, ensembles...). Les règles de manipulation admises ajoutées aux axiomes d'une théorie mathématique permettent-elles de déduire toutes les propositions vraies pour toute structure vérifiant les axiomes ? Plus simplement, peut-on démontrer tout ce qui est vrai pour toutes les interprétations des symboles ?

La réponse attendue était oui, et Gödel le confirme dans sa thèse intitulée *La complétude du calcul des prédicats du premier ordre*, où il établit que les principes de la logique prouvent tout ce qui est vrai à partir d'un ensemble d'axiomes donné. Cependant, il ne démontre pas que les axiomes alors admis pour la théorie des nombres permettent de démontrer toutes les propositions à propos des nombres. Les axiomes de la théorie des nombres avaient été proposés par le

mathématicien italien Giuseppe Peano (1858-1932) en 1889 ; ils incluent l'axiome de récurrence, qui affirme que toute propriété vraie pour zéro, et vérifiée par le nombre $n+1$ lorsqu'elle est vraie pour le nombre n , est vraie pour tout entier naturel. Cet axiome semble évident, mais il gêne les mathématiciens parce qu'il concerne les propriétés des nombres plutôt que les nombres eux-mêmes : c'est un axiome du second ordre, qui semble trop éloigné des nombres pour définir ces derniers. De la même manière, savoir qu'un ballon est bleu n'indique pas ce qu'est un ballon.

L'axiome de récurrence avait été reformulé sous la forme d'un groupe infini d'axiomes identiques, qui se rapportaient à des formules spécifiques plutôt qu'aux propriétés générales des nombres. Malheureusement, le logicien norvégien Thoralf Skolem avait démontré que ces axiomes ne caractérisent pas seulement des nombres naturels : ils sont également vérifiés par d'autres structures nommées entiers non standards.

Le théorème de complétude de Gödel indique que l'on peut démontrer toutes les propositions qui découlent des axiomes ; cependant une proposition qui est vraie pour les nombres naturels, mais fausse pour un autre système d'éléments qui vérifient les mêmes axiomes, est alors indémontrable (voir l'encadré). Les mathématiciens dédaignent la restriction en espérant qu'il n'existe pas d'entités similaires aux nombres.

L'article que Gödel publie en 1931 bouleverse alors les mathématiques. Il

montre que certaines propositions vraies pour les nombres naturels sont indémonstrables : il existe des objets qui vérifient les axiomes de la théorie des nombres, mais se comportent différemment à d'autres égards. En prenant toutes les propositions vraies pour axiomes, on contournerait ce « théorème d'incomplétude » ; mais alors comment savoir si les propositions sont vraies ? Gödel montre que, lorsque les axiomes sont décrits par un ensemble de règles mécaniques, le choix des axiomes n'évite pas la difficulté : quand elles sont vraies pour les nombres naturels, d'autres propositions vraies sur ces nombres restent indémonstrables.

Par exemple, lorsque les axiomes ne se contredisent pas mutuellement, cette non-contradiction, correctement codée en une proposition numérique, est formellement indécidable, c'est-à-dire ni démontrable ni réfutable à partir des axiomes. La démonstration de la non-contradiction nécessite donc des principes plus puissants que les axiomes eux-mêmes.

Ce dernier résultat ruine le programme de David Hilbert, qui voulait renforcer les fondements des mathématiques et déduire la cohérence des théories mathématiques complexes de celle de théories plus simples. Pour Gödel, en revanche, les théorèmes d'incomplétude ne réfutent pas l' inanité de la méthode axiomatique, mais ils montrent que la démonstration de théorèmes ne peut être complètement mécanisée et ils justifient l'intuition en mathématique.



2. LE COUPLE ADÈLE PORKERT ET KURT GÖDEL était très uni. Ils sont ici à la terrasse d'un café de Vienne, pendant leurs longues fiançailles. Adèle Porkert protégeait Gödel de ses seurs irrationnelles et était souvent la seule personne à pouvoir le convaincre de manger. Plus que quiconque, elle a contribué à le maintenir en vie et en état de travailler.