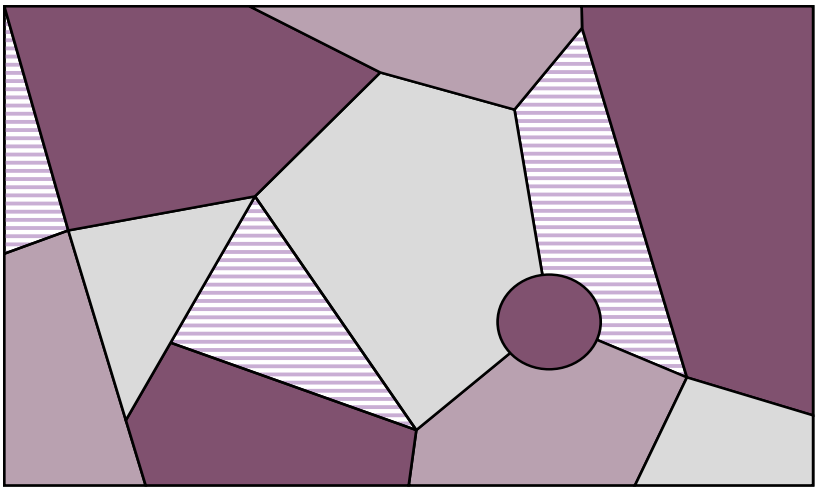
LE THÉORÈME DES QUATRE COULEURS EST DÉMONTRÉ

En 1852, Francis Guthrie, mathématicien et botaniste sud-africain, a postulé que quatre couleurs suffisent à colorier n'importe quelle carte plane en s'assurant que deux pays ayant une frontière commune soient de couleurs différentes. Le résultat semblait d'autant plus évident que, bien souvent, trois couleurs suffisent et que, en 1890, une preuve simple a été trouvée pour cinq couleurs. Pourtant, pendant près d'un siècle, toutes les preuves que quatre couleurs suffisent se sont révélées fausses.

En 1977, à la suite des travaux de l'Allemand Heinrich Heesch, Kenneth Appel et Wolfgang Haken, de l'université de l'Illinois, ont démontré que s'il devait y avoir un contre-exemple, il appartiendrait à un ensemble de 1936 cas «critiques» possibles (plus tard réduit à 1478). Ils ont alors écrit un programme informatique qui a réussi – en tâtonnant – à colorier ces 1936 cas avec quatre couleurs seulement: une vérification impossible à la main et qui a pris à l'époque plus de 1200 heures de calculs! Le théorème des quatre couleurs était donc démontré? À voir...

Ce tout premier cas de preuve informatique consistant non pas à prouver un théorème par le raisonnement, mais à tester puis à rejeter un nombre fini mais colossal de contre-exemples fit scandale à l'époque. En 2005, Georges Gonthier et Benjamin Werner, à l'Inria (Institut national de recherche en informatique et automatique), ont reproduit les résultats d'Appel et Haken à l'aide d'un logiciel assistant de preuve (où le raisonnement est formalisé dans ses moindres détails, de telle façon qu'il soit vérifiable par tous), mettant ainsi fin à la polémique. L'informatique est devenue depuis un outil légitime de la recherche et de la formulation de preuves en mathématique. ■



Quatre couleurs suffisent pour colorier une carte de telle sorte que deux pays ayant une frontière commune soient toujours de couleurs différentes (en supposant que tous les pays sont faits d'un seul morceau, sans enclave).

RENÉ CUILLIERIER
journaliste scientifique

K. Appel et W. Haken, *Illinois Journal of Mathematics*, vol. 21, pp. 429-490, 1977

LA CRYPTOGRAPHIE À CLÉ PUBLIQUE VOIT LE JOUR

Depuis l'Antiquité, pour échanger des messages secrets, il fallait au préalable que l'auteur et son destinataire se mettent d'accord sur une méthode de chiffrement. Hélas, si un tiers interceptait cet échange, leurs efforts de discrétion étaient réduits à néant.

En 1976, Whitfield Diffie et Martin Hellman, alors à l'université Stanford, ont proposé l'idée d'une «cryptographie à clé publique» ou «asymétrique». Une analogie l'illustre. Alice (le destinataire) envoie à Bernard (l'émetteur) un coffre ouvert (la clé publique) dont elle seule a la combinaison (la clé secrète). Bernard introduit le message dans le coffre, le ferme et le réexpédie à Alice qui est alors la seule à pouvoir y accéder, quand bien même le coffre serait intercepté avant de lui parvenir. Whitfield Diffie et Martin Hellman n'avaient pas donné d'algorithme mettant ce principe en pratique, mais, en 1978, Ronald Rivest, Adi Shamir et Leonard Adleman y sont parvenus à partir de résultats de la théorie des nombres, ce qui a donné l'algorithme RSA. La fonction publique f qui produit le message chiffré, $f(M)=C$, est choisie de telle façon que f^{-1}, sa réciproque qui redonne le message initial, $f^{-1}(C)=M$, soit presque impossible à calculer. Dans l'algorithme RSA, la fonction est construite à partir de deux nombres premiers p et q, sachant qu'il est facile de les multiplier pour obtenir $n=p\times q$, mais que trouver les facteurs premiers p et q à partir de la seule connaissance de n nécessite un temps de calcul rédhibitoire si les entiers sont très grands.

La cryptographie asymétrique est aujourd'hui à la base de presque tous les échanges de données sécurisés sur Internet. ■

1 024

C'EST LE NOMBRE DE BITS QUI CODENT LES PLUS PETITES CLÉS PUBLIQUES ACTUELLES. CELA CORRESPOND À DES NOMBRES D'ENVIRON 256 CHIFFRES DÉCIMAUX.

R. C.

R. L. Rivest *et al.*, *Comm. of the ACM*, vol. 21(2), pp. 120-126, 1978