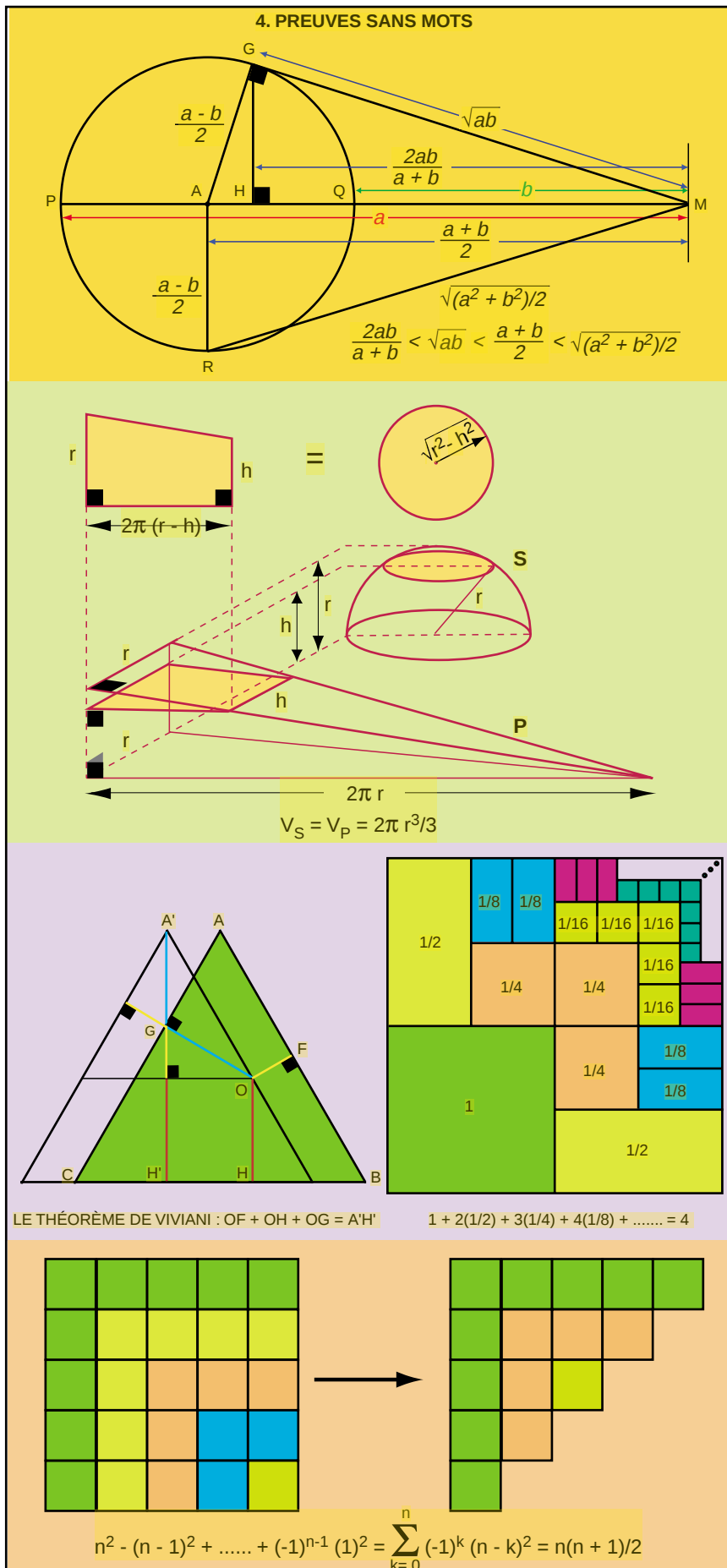


Ces facilités autorisées par les «lais-sés au lecteur», et autres «à titre d'exem-ple, démontrons le cas numéro 5», sont dangereuses, car tous ceux qui écrivent des textes mathématiques savent que bien souvent ils n'ont pas détaillé pour eux-mêmes sur une feuille à part ces parties manquantes qu'ils suggèrent au lecteur de reconstituer seuls. Ils y ont réfléchi, ils sont intimement convaincus que «ça passe», mais est-ce suffisant ? Pour-tant comment pourrait-on s'interdire ces facilités, puisque Bourbaki lui-même reconnaît que, dans les textes mathé-matiques, «l'emploi des ressources de la rhétorique est nécessaire» (Bourbaki, Introduction, p. 7) ?

Encouragé par le plaisir de l'écono-mie et l'élégance de la concision, sou-cieux aussi de ne pas passer pour un imbécile en donnant des détails sur un passage vraiment facile, tout mathé-maticien écourte ses démonstrations, et cela d'autant plus qu'il s'adresse à des mathématiciens de haut niveau. Assez étrangement donc, les risques sont maxi-maux dans les textes présentant des résultats de recherches. Dans un cours destiné à des étudiants, le mathéma-ticien essaiera de contenir son penchant pour les brèves esquisses de preuves, sans toutefois résister à la tentation d'un «le cas 1 est trivial» et surtout au coup de l'exercice. Ces laconiques pirouettes font le désespoir des étudiants moyens, incapables de boucher ces trous pré-tendument aisés, et donnent un senti-ment de culpabilité au lecteur trop pressé qui se dispense des travaux suggérés, dont pourtant, dans l'introduction, l'au-teur a indiqué, avec perfidie, qu'il était important de les traiter soigneusement pour s'assurer de la bonne assimilation du cours.

UN TROU FAMEUX

Un des plus fameux trous dans une preuve mathématique provient d'un de ces rac-courcis imprudents. On sait que, le mer-credi 23 juin 1993, à l'issue de trois jours de conférence Andrew Wiles concluait en public une présentation de la preuve du Grand Théorème de Fermat (qu'il démon-trait comme cas particulier de résultats plus généraux). Personne sur le coup ne put vérifier la démonstration bien trop com-plexe, dont seules les grandes lignes avaient été expliquées oralement. La démonstration, d'environ deux cents pages, fut soumise à un comité d'experts com-posé de six spécialistes qui travaillèrent des mois durant. De nombreuses fois, ils durent interroger A. Wiles pour obtenir des explications leur permettant de saisir le sens de ce qui était écrit. Face à une preuve formelle, les experts mathématiciens n'au-



5. PREUVE HEURISTIQUE IMPOSSIBLE (AUJOURD'HUI) À TRANSFORMER EN PREUVE FORMELLE

On considère la suite des nombres entiers définie par :

$$x_1 = 2,$$

$$x_2 = [\text{le plus petit facteur premier de } x_1 + 1] = 3,$$

$$x_3 = [\text{le plus petit facteur premier de } x_1 x_2 + 1] = 7, \dots,$$

$$x_{n+1} = [\text{le plus petit facteur premier de } x_1 x_2 \dots x_n + 1], \dots$$

Le début est 2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, ...

Cette suite d'Euclide-Mullin n'énumère que des nombres premiers différents. En effet, $y_n = x_1 x_2 \dots x_n + 1$ n'est pas divisible par x_1 (sinon 1 le serait comme différence de deux nombres divisibles par x_1). Le nombre y_n n'est pas divisible par x_2 (sinon 1 le serait), etc. Puisque y_n n'est divisible par aucun des nombres premiers, $x_1, \dots, x_n$, x_{n+1} est un nouveau nombre premier, et donc tous les x_i sont des nombres premiers distincts. La question est de savoir si cette suite énumère tous les nombres premiers sans en oublier (bien sûr, ce sera dans le désordre). On pense que oui et l'on propose la preuve heuristique suivante.

Supposons que la suite ne contienne pas tous les nombres premiers. Soit p le plus petit nombre premier qui n'est pas dans la suite. À partir d'un certain N , tous les nombres premiers inférieurs à p seront parmi les nombres $x_1, \dots, x_N$. Si n est un entier quelconque plus grand que N , le nombre $y_n = x_1 x_2 \dots x_n + 1$ peut être considéré comme un nombre quelconque vis-à-vis de p , et donc ce nombre a une chance sur p d'être un multiple de p (car un entier sur p est multiple de p). Le nombre y_n a donc une probabilité de $(1-1/p)$ de n'être pas multiple de p , qui est aussi la probabilité que x_{n+1} soit différent de p . La probabilité pour que ni $x_N + 1$ ni $x_{N+2} \dots x_{N+k}$ ne soient égaux à p est donc $(1-1/p)^k$ qui tend vers 0 à l'infini. Autrement dit, la probabilité pour que p n'apparaisse pas dans la suite x_n est nulle. Donc p apparaît dans la suite, ce qui contredit sa définition. Donc, tout nombre premier p apparaît dans la suite x_n , qui n'est pas autre chose que la liste des nombres premiers, sans répétition et écrite dans le désordre.

Un tel raisonnement est presque bon, mais il suppose que y_n est tiré au hasard, ce qui n'est pas le cas, et donc, sans un complément (que personne n'a réussi à découvrir et qui semble hors de portée des méthodes mathématiques actuelles), la preuve heuristique n'est pas une preuve acceptable.

raient pas eu à contacter A. Wiles ! A. Wiles lui-même prétendait avoir vérifié chaque étape de la démonstration deux fois avant de la confier à ses collègues. À chaque question des experts, il proposait d'ailleurs une réponse qui levait la difficulté soulevée. Petit à petit, A. Wiles rendait compréhensible son document, qui, si les mathématiciens se conformaient à la description idéalisée évoquée au début de cet article, aurait dû l'être dès le départ.

On avançait lentement vers une validation totale, jusqu'au jour où une réponse ne contenta pas totalement un expert, ni le complément de réponse du jour suivant : il y avait un trou dans la démonstration, que, malgré tout le soin pris par A. Wiles, ce dernier n'avait pas vu. Le « bogue » provenait de l'utilisation, hors des conditions précises où il avait été démontré, d'un procédé que A. Wiles, dans une généralisation hâtive, avait utilisé sans faire dans ce cas tous les contrôles exigés.

On connaît la suite : plus de deux ans furent nécessaires pour corriger l'erreur et arriver, en empruntant un chemin différent de celui proposé en 1993, à une démonstration complète et accep-

tée des experts. Notons, pour rassurer les inquiets, qu'une fois cet accord des experts obtenu, la preuve fut confirmée par d'autres experts. Plus aucun doute ne persiste aujourd'hui sur sa validité, c'est-à-dire sur la possibilité d'écrire une preuve formelle du théorème de Fermat. La longueur de la preuve interdit, pour l'instant, cette transcription formelle complète, mais il n'y a aucune controverse sur son existence. La difficulté évoquée dans la rubrique de novembre concernant la transcription de la preuve de A. Wiles dans le formalisme de l'arithmétique élémentaire de Peano (plus limité que celui de la théorie des ensembles qui sert de référence implicite aujourd'hui) n'entache en rien l'unanimité qui règne sur la validité de la preuve de A. Wiles, et, sauf à imaginer que la théorie des ensembles est contradictoire, la victoire est définitive.

LES CONTROVERSES

Aujourd'hui, lorsqu'il y a une controverse en mathématiques sur la validité d'une démonstration, il est donc vrai en défini-

tive qu'elle ne dure jamais longtemps, et cela à cause de la possibilité de s'approcher de plus en plus de ce que serait la preuve formelle complète du résultat.

Le rapport entre *preuves formelles* et *preuves réelles* peut donc se résumer en disant : les preuves formelles ne sont que très rarement écrites par les mathématiciens parce qu'elles sont très longues, mais ce sont quand même elles qui servent de recours ultime dans l'évaluation d'une *preuve réelle* dont la validité est douteuse. C'est, en effet, en cherchant à s'approcher pas à pas de ce que serait la *preuve formelle* du résultat discuté qu'on obtient l'accord définitif : ou bien on ne rencontre pas d'obstacles sur le chemin qui y conduit (et qu'on emprunte rarement jusqu'au bout) et la *preuve réelle* est considérée juste, ou bien un trou insurmontable apparaît et la preuve est insuffisante, donc inexistante...

La suppression des controverses en mathématiques est relativement nouvelle, car, avant les progrès logiques du début du siècle, il s'en présentait régulièrement et de graves incertitudes divisaient les esprits, même en mathématiques. Ce fut le cas à la fin du XVIII^e siècle quand le calcul différentiel fut découvert et que la notion de limite n'était qu'imparfaitement maîtrisée (elle le fut par A. Cauchy, 1789-1857, et par K. Weierstrass, 1815-1897). Au moment de la mise au point de la topologie, d'autres controverses prolongées eurent lieu, comme celle que le philosophe Imre Lakatos détaille dans son livre à propos de la formule d'Euler $s - a + f = 2$ (a est le nombre d'arêtes d'un polyèdre ; s le nombre de sommets ; f le nombre des faces) dont il fut difficile de préciser exactement le domaine de validité.

Au début du siècle, une des dernières grandes controverses en mathématiques fut celle concernant les fondements mais elle ne porta pas sur l'exactitude ou l'inexactitude de preuves précises, ce fut une discussion sur les modes de raisonnement qu'on pouvait légitimement mettre en œuvre (notions ensemblistes, axiome du choix, raisonnements non constructifs, etc.). Aujourd'hui, grâce aux systèmes formels, la controverse sur les fondements des mathématiques s'est éteinte et n'est plus qu'un problème pour philosophes dont peu de mathématiciens se soucient. Sur toute question importante, un accord unanime s'établit, ce qui fait véritablement des mathématiques une science à part.

Des doutes concernant le théorème de Gödel exprimés juste après sa parution par quelques mathématiciens et les incompréhensions graves qui font douter des amateurs de tel ou tel résultat