2. LE LAISSER-ALLER TUE UNE ÉCOLE MATHÉMATIQUE

Jamais en mathématiques on ne peut baisser sa garde, car alors l'erreur fond sur vous et vous fait perdre tout crédit. L'école de géométrie algébrique italienne (dont on avait fini par penser qu'elle fournissait simultanément une démonstration d'un résultat et un contre-exemple) est un cas étonnant d'abandon fatal de la rigueur. Le mathématicien David Mumford explique cette histoire étrange :

«Il existe des exemples d'erreurs mathématiques graves du type suivant : une école de mathématiques se détourne du droit chemin, et après avoir donné des preuves rigoureuses se laisse lentement gagner par de mauvaises habitudes, jusqu'à ce que des faussetés évidentes soient publiées. Bien sûr, le reste du monde, après s'être laissé abuser, devient progressivement méfiant, puis finalement met le doigt sur des erreurs dans les textes imprimés par les membres de l'école. Le cas le plus connu de cette situation est celui de l'école italienne de géométrie algébrique, qui produisit d'excellents et profonds résultats pendant 50 ans, mais s'effondra ensuite. Trois noms clefs doivent être cités : Castelnuovo, Enriques et Severi. Castelnuovo le plus ancien était un splendide mathématicien parfaitement rigoureux. Enriques qui vient après lui, autant que je le sache, ne publia jamais rien de faux, quoiqu'il reconnaissait que certaines de ses démonstrations ne traitaient pas vraiment tous les cas possibles. Il avait ses propres critères, mais acceptait volontiers de réexaminer une "démonstration" et de la rendre plus complète. Malheureusement Severi, le troisième, qui était fasciste et possédait un tempérament autoritaire, tua finalement l'école entière, car bien qu'ayant débuté par une série de découvertes brillantes et correctes, il publia dans les années 1930 et 1940 des livres remplis d'erreurs. Le reste du monde devint hésitant sur ce qui avait été vraiment prouvé par toute cette école. Il fallut les efforts de deux grands hommes, Zariski et Weil, pour remettre les choses en ordre.»

1880, le mathématicien Landry montrera que $F_6 = 274177 \times 67280421310721$. On sait aujourd'hui que, de F_5 à F_{30}, tous les F_n sont composés et on conjecture que tous les nombres de la forme $2^{2^n}+1$ sont composés, sauf les quatre premiers!

Ces erreurs ne sont pas très instructives : une fois repérées, rien n'en découle. Ce n'est pas le cas de celle commise à propos du «petit théorème de Fermat». Ce résultat, énoncé par Fermat en 1640 et démontré par Euler en 1736, indique que si p est un nombre premier, alors pour tout nombre entier a supérieur à 1, le nombre $a^p - a$ est un multiple de p. Ainsi, en particulier, si p est premier, $2^p - 2$ est un multiple de p. Cette affirmation ne doit pas être confondue avec l'affirmation inverse qui est fausse : si $2^p - 2$ est un multiple de p, alors p est premier. Fermat ne commit pas la confusion, pourtant tentante. En effet, les nombres qui font exception, c'est-à-dire qui vérifient que $2^p - 2$ est un multiple de p alors qu'ils sont composés (on les appelle 2–pseudo-premiers) sont très rares. Le plus petit est $341 = 11 \times 13$. En choisissant au hasard un nombre n inférieur à 25 milliards, on constate : *(a)* que $2^n - 2$ n'est pas multiple de n dans 95,64 pour cent des cas (on sait alors avec certitude qu'il est composé) ; *(b)* que $2^n - 2$ est multiple de n dans 4,36 pour cent des cas et alors n est un nombre premier dans 99,998 pour cent des cas. Pour un nombre inférieur à 25 milliards, le risque d'établir un diagnostic faux à partir de la croyance (erronée) que «n est premier si et seulement si $2^n - 2$ est multiple de n» est inférieur à 0,00009 pour cent. La croyance erronée tendait les bras et, en 1886, le mathématicien chinois Li Shan-Lan (1811-1882) a publié ce faux critère. Le plus remarquable est qu'aujourd'hui cette croyance fausse (un peu améliorée pour l'être moins souvent encore) sert de base aux algorithmes probabilistes de test de primalité qui sont utilisés systématiquement en cryptographie. Personne ne commet vraiment d'erreur, cependant c'est bien de la fausse caractérisation qu'est née l'idée des algorithmes probabilistes, si importante aujourd'hui. De l'erreur (contrôlée et consciente), on a tiré une méthode importante et utile.

LES FAUSSES DÉCIMALES DU NOMBRE π

Avant l'ère des ordinateurs, quelques problèmes de calculs ont excité les passions et ont été l'occasion d'erreurs à répétition. Ainsi le calcul à la main des décimales de π a donné lieu à une multitude d'erreurs, dont la plus célèbre laisse des marques aujourd'hui encore.

William Shanks (1812-1882) publie 707 décimales de π en 1874. Au total, il a passé 20 ans de sa vie à mener ce calcul et heureusement… n'a jamais su qu'il était faux à partir de la 527e décimale. Pendant plus de 50 ans d'ailleurs tout le monde fit confiance au calcul de Shanks. C'est seulement en 1945 que D. Ferguson, travaillant comme Shanks uniquement avec du papier et des crayons, recalcule 539 décimales de π et constate un désaccord avec le calcul de son prédécesseur. Le désaccord sera confirmé plus tard, par d'autres calculs utilisant cette fois des machines. Les chiffres faux de Shanks furent utilisés en 1937 pour l'aménagement du Palais de la découverte à Paris. La salle π du Palais vit son plafond décoré par les décimales de Shanks. Les fausses décimales de π restèrent jusqu'en 1949 date à laquelle les bons chiffres furent mis en place. On pourrait croire que depuis les fausses décimales de Shanks ont été oubliées. Ce n'est pas le cas : l'éditeur français Hermann en 2001 vend toujours le merveilleux livre de François Le Lionnais *Les grands courants de la pensée mathématique*, livre qui, page 99, reproduit sans indiquer qu'elles sont fausses, les 707 décimales de Shanks. Ne les apprenez pas par cœur!

L'erreur de Shanks est sans importance matérielle puisque l'on sait bien qu'en physique 40 décimales de π seront toujours suffisantes. Il n'empêche que suite aux erreurs répétées dans la course aux décimales de π (aujourd'hui on en connaît 206 milliards), les règles du jeu sont maintenant qu'un calcul doit être réalisé deux fois par deux méthodes différentes pour être pris en considération. Ici l'erreur a incité à la prudence.

LES MATHÉMATIQUES ERRONÉES DU JEU

Les erreurs mathématiques ne sont pas toujours aussi indolores. On raconte que le Chevalier de Méré (1607-1684), qui était philosophe et curieux des sciences, possédait un goût prononcé pour les jeux de hasard. Il recherchait des règles astucieuses et en tirait des paris qu'il proposait à tous. L'une des règles qu'il inventa consiste à faire rouler quatre dés et à parier à un contre un sur l'apparition d'au moins un 6. La probabilité de perdre est $(5/6)^4 = 625/1296$, soit 48,225 pour cent, ce qui donne donc un léger avantage à celui qui propose le jeu et l'assure à la longue de gagner… beaucoup d'argent. Méré inventa une autre règle : lancer deux dés 24 fois de suite et parier que le double 6 apparaîtra au moins une fois. Cette fois, le calcul, que nous savons faire aujourd'hui, donne que la probabilité de perdre pour celui qui offre le pari, est $(35/36)^{24} = 50{,}859$ pour cent (pour que l'avantage soit à celui qui propose le pari, il faudrait changer le 24 en 25). Le Chevalier était donc condamné à la longue à perdre de l'argent avec ce second jeu.

La légende veut que le Chevalier de Méré après avoir gagné une fortune grâce au premier jeu, la perdit en pratiquant le second. Cette erreur d'appréciation et quelques autres du même type eurent des conséquences plus importantes que celles, pécuniaires, que subit le Cheva-