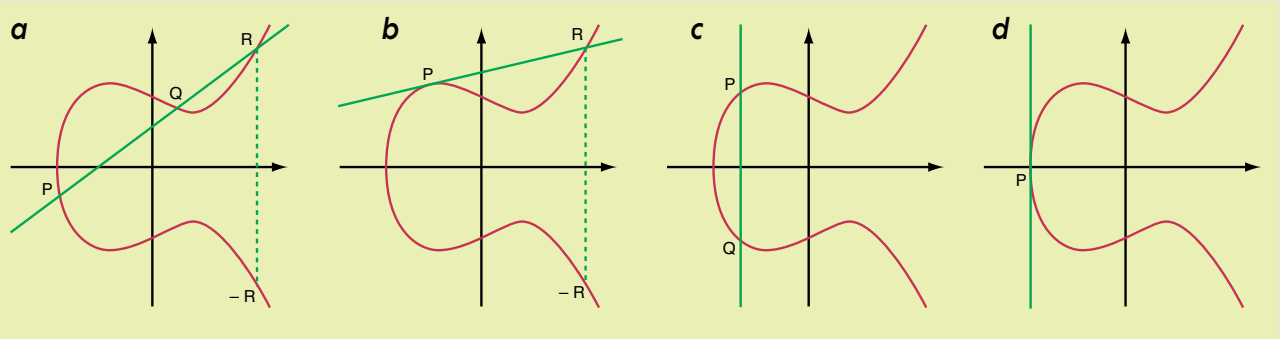
COURBES ELLIPTIQUES ET LOI DE GROUPE

Les courbes elliptiques sont un des outils clés de la démonstration du théorème de Fermat par Andrew Wiles. Voyons de plus près leurs caractéristiques. Une courbe elliptique E est une courbe de genre 1 dont l'équation se ramène à : $y^2+axy+by=x^3+cx^2+dx+e$, où a, b, c, d et e sont des entiers. Une telle équation définit une courbe de genre 1 si elle n'a pas de points singuliers, c'est-à-dire si les dérivées partielles par rapport à x et à y de l'équation ne s'annulent pas en même temps (ce qui impose une condition sur les coefficients). Un point de la courbe E est n'importe quel couple de nombres complexes vérifiant l'équation associée. Si certains points ont des coordonnées réelles (respectivement rationnels), on dit qu'ils sont réels (rationnels). Une propriété cruciale des courbes elliptiques est la suivante : l'ensemble de leurs points forme un groupe commutatif, et il en est de même pour l'ensemble de leurs points réels et celui de leurs points rationnels. En d'autres termes, l'« addition » ou la « soustraction » de deux points de la courbe donne un point de la courbe. Qu'est-ce que l'addition de deux points ? Considérons par exemple la courbe elliptique d'équation : $y^2=x^3-x-1$, et deux points distincts P et Q sur cette courbe *(voir la figure)*. La droite qui les joint recoupe en général la courbe en un troisième point R. On définit la somme des points P et Q comme étant le point symétrique de R par rapport à l'axe des abscisses. Si P=Q, on utilise la tangente à la courbe : le point P+P=2P est le symétrique par rapport à l'axe des abscisses du point d'intersection de la tangente en P avec la courbe. L'opposé d'un point P, noté – P, est le symétrique de P par rapport à l'axe des abscisses. Et l'élément neutre du groupe commutatif est le point , point de rencontre des verticales à l'infini. Ainsi, la somme de P et de son opposé est bien nulle, puisque la droite qui joint ces points est verticale. Autre propriété importante des courbes elliptiques : elles présentent des points de torsion, c'est-à-dire des points dont un multiple entier est nul. Pour un entier $n>2$, l'ensemble E[n] des points à coordonnées complexes de la courbe E dont le n-ième multiple est 0 (les points de n-torsion), associés au point ∞, l'élément neutre, constitue un groupe commutatif dit de n-torsion.

On montre, à partir de l'expression des coordonnées de la somme de plusieurs points, que les abscisses x des points de E[n] vérifient une équation polynomiale à coefficients rationnels. Or, par définition, le groupe de Galois absolu conserve les relations algébriques, en particulier l'équation vérifiée par les abscisses des points de E[n], et celle vérifiée par leurs ordonnées – l'équation de E. Par conséquent, il permute les points de E[n] entre eux. C'est grâce à cette propriété que l'on peut établir une correspondance entre le groupe E[n] et le groupe de Galois absolu. On a ainsi construit une représentation galoisienne des courbes elliptiques. Andrew Wiles démontra la conjecture de Shimura-Taniyama-Weil en établissant une correspondance similaire entre le groupe de Galois absolu et les fonctions modulaires, et en montrant que ces deux représentations galoisiennes sont isomorphes.

Catherine Goldstein, institut de mathématiques de Jussieu-Paris-Rive-gauche.



Différents cas d'addition de points *P* et *Q* sur la courbe elliptique d'équation $y^2=x^3-x-1$, représentée dans le plan réel. Quand P et Q sont distincts, P+Q=–R (*a*). Quand P=Q, P+P=–R (*b*). Quand P et Q ont la même abscisse (*c*), leur somme est égale au point ∞ (là où les droites verticales se rencontrent à l'infini). Quand P et Q sont confondus en un point de tangente verticale, P+P vaut le point ∞ (*d*).

démonstration de Faltings exploite la résolution, due à Pierre Deligne en 1978, de la conjecture de Weil. André Weil avait proposé en 1949 un analogue pour les corps finis de la célèbre hypothèse de Riemann, formulée à l'origine pour le corps $\mathbb{C}$ des nombres complexes (*voir L'hypothèse qui valait un million, par P. Meier, page 68*).

DÉTOUR PAR LE JAPON

Ainsi aucune équation du type (2) ne peut avoir un nombre infini de solutions génératrices pour $n>2$. Peu après, en 1985, en utilisant le résultat de Faltings, Andrew Granville et Roger Heath-Brown démontrèrent que le nombre de solutions des équations (2), s'il en existe, est une fonction décroissante de l'entier n. Ce point ne résout cependant pas l'énigme de Fermat. Il suffit en effet d'une seule solution rationnelle de l'équation (2) pour obtenir une solution entière de l'équation (1) et donc un nombre infini de solutions de celle-ci.

La solution de l'énigme de Fermat fut finalement l'œuvre d'un descendant de la vieille Angleterre émigré aux États-Unis, Andrew Wiles. Le chemin tortueux de la découverte passa par le Japon tumultueux de l'après-guerre. Revenons au cas $n=2$ du théorème, exprimé au moyen de l'équation (3) : $x^2+y^2=1$. On peut paramétriser x et y par respectivement les fonctions cosinus et sinus, qui satisfont la relation : (4) $\cos^2\alpha+\sin^2\alpha=1$.

Résoudre l'équation de Fermat pour $n=2$, c'est-à-dire déterminer les triplets de Pythagore, >

revient donc à trouver un angle α dont le sinus et le cosinus sont des rationnels. En 1955, le Japonais Yutaka Taniyama énonça une conjecture qui généralisait cette idée aux courbes elliptiques définies sur $\mathbb{Q}$. Ces courbes, ainsi nommées parce qu'elles interviennent dans la rectification d'un segment d'ellipse, sont les courbes de genre 1 dont l'équation peut se ramener à une expression du type : $y^2+axy+by=x^3+cx^2+dx+e$, où a, b, c, d et e sont des entiers (*voir l'encadré page précédente*). Taniyama conjectura que ces courbes peuvent être paramétrisées par certaines fonctions dites modulaires qui généralisent les fonctions trigonométriques. On retrouva Taniyama, âgé d'à peine 31 ans, mort dans son appartement le matin du 17 novembre 1958. Dans une lettre laissée sur son bureau, il confiait son intention de mettre fin à ses jours.

Précisée par André Weil en 1968 et reprise en 1971 par un autre Japonais, Goro Shimura, cette conjecture prit le nom de « conjecture de Shimura-Taniyama-Weil ». Pour le mathématicien japonais, elle est inspirée par l'idée de la bonté intrinsèque des mathématiques. Quel lien existe-t-il entre cette conjecture et le dernier théorème de Fermat ?

En 1985, l'Allemand Gerhard Frey propose d'associer la courbe elliptique d'équation (5) : $y^2=x(x+a^n)(x-b^n)$ à un triplet de Fermat (a, b, c), c'est-à-dire un triplet vérifiant l'équation (6) : $a^n+b^n=c^n$ (en supposant qu'il en existe pour un quelconque n).

L'équation (5) est belle, mais infidèle : selon Frey, cette courbe représenterait un contre-exemple de la conjecture de Shimura-Taniyama-Weil. Il serait impossible de la paramétriser avec des fonctions modulaires. La conjecture de Frey (connue sous le nom de « conjecture epsilon ») est une métaconjecture, c'est-à-dire une conjecture selon laquelle si une autre conjecture est vraie (la conjecture de Shimura-Taniyama-Weil) alors le théorème de Fermat l'est aussi.

Un an plus tard, l'Américain Kenneth Ribet démontre que la courbe de Frey n'est pas paramétrisable par des fonctions modulaires. Pour résoudre l'énigme de Fermat, il « suffit » donc à présent de démontrer la prémisse de la conjecture epsilon, c'est-à-dire la conjecture de Shimura-Taniyama-Weil.

LA FIN HEUREUSE D'UNE ÉPOPÉE

On pourrait penser que l'énigme n'a été que simplement déplacée, mais, comme Andrew Wiles le souligne en 1993, travailler sur les courbes elliptiques modulaires, objets géométriques sur lesquels on sait déjà beaucoup et on espère en savoir encore plus, est bien différent de travailler avec les propriétés des nombres, que Fermat qualifiait de fugitives.

La preuve de Wiles s'insère dans ce contexte précis. En premier lieu, il restreint l'analyse de la conjecture de Shimura-Taniyama-Weil en se limitant à la classe des courbes elliptiques dites semi-stables, classe à laquelle appartient la courbe d'équation (5).

La grande intuition de Wiles consiste à faire appel à un outil fondamental des mathématiques, la théorie des groupes de Galois (*voir l'encadré page 101*). Au XIXe siècle, le jeune Évariste Galois a établi une correspondance entre les fonctions rationnelles des solutions d'une équation et le groupe des permutations de ces solutions. L'avantage de cette traduction est qu'un groupe est souvent une structure engendrée par un ensemble fini d'éléments. Wiles propose de comparer les représentations de Galois correspondant aux courbes elliptiques semi-stables avec celles correspondant aux fonctions modulaires.

UN TROU DANS LA DÉMONSTRATION

En 1993, au cours d'une rencontre à l'institut de mathématiques de Cambridge, en Angleterre, il annonce y être parvenu. Mais quelques mois plus tard, en décembre, il reconnaît que sa démonstration présente un « trou ». Rentré à Princeton, il se met au travail pour corriger la faille. En octobre 1994, il annonce en être venu à bout en collaboration avec un ex-étudiant de Cambridge, Richard Taylor.

En mai 1995, un long texte de Wiles, intitulé « Modular elliptics curves and Fermat's last theorem » (« Les courbes elliptiques modulaires et le dernier théorème de Fermat ») et contenant le cœur de son raisonnement, paraît dans la revue *Annals of Mathematics*, suivi d'un autre article écrit en collaboration avec Richard Taylor, « Ring theoretic properties of certain Hecker algebras » (« Les propriétés théoriques annulaires de certaines algèbres de Hecker »), qui apporte la solution du point critique. Finalement, en 1999, Taylor, avec Brian Conrad, Christophe Breuil et Fred Diamond complètent le travail de Wiles en montrant que la conjecture de Shimura-Taniyama-Weil est aussi valide pour les courbes elliptiques non semi-stables.

Le dernier théorème de Fermat, qui découle de la conjecture de Shimura-Taniyama-Weil, est enfin démontré. L'épopée séculaire, commencée dans une marge trop étroite, est close. Comme l'écrivit François Rabelais (1494-1553), mieux vaut conclure les controverses par des signes que par des déclamations lorsqu'on recourt à des arguments si compliqués que les paroles humaines ne peuvent suffire à les exposer correctement. C'est pourquoi, après tant d'épisodes personnels bizarres ou dramatiques, la résolution de l'énigme de Fermat confirme le mot du mathématicien américain Hans Lewy : « L'histoire des mathématiques n'est ni tragique ni comique, mais épique. » ■

BIOGRAPHIE

N. VERDIER, *Galois : le mathématicien maudit*, Belin-Pour la Science, 2011.

R. TAYLOR et A. WILES, Ring-Theoretic Properties of Certain Hecke Algebras, *Annals of Mathematics*, vol. 141, pp. 553-572, 1995.

A. WILES, Modular Elliptic Curves and Fermat's Last Theorem, *Annals of Mathematics*, vol. 141, pp. 443-551, 1995.

C. GOLDSTEIN, Autour du théorème de Fermat, *Mnémosyne* n° 7, pp. 34-61, 1994.

Des nombres et des énigmes

Les dernières énigmes préparées par Ana Retchman et Sébastien Kernivinen.

Solutions page 106.


Ana Retchman


Sébastien Kernivinen

ÉNIGME 10

Trouver le plus petit nombre divisible par 999 qui ne contienne pas de 9 parmi ses chiffres.

ÉNIGME 11

Calculer la somme de tous les nombres palindromes à 3 chiffres.

ÉNIGME 12

Si p et p^2+8 sont des nombres premiers, quelle est la valeur de p^3+4 ?

ÉNIGME 13

Combien de chiffres a le plus petit nombre entier qui se termine par 2 tel que si on déplace le chiffre 2 en tête du nombre on obtient un nombre deux fois plus grand ?

ÉNIGME 14

Écrire le nombre 2 019 sous la forme d'une somme de cinq nombres entiers au cube.

Réponses et solutions

Réponse 1: $N=8$

Solution. On dira que deux nombres sont *cotassés* lorsque chacun d'eux, ainsi que leur somme, sont coloriés d'une même couleur. En coloriant les nombres de [1, 8] ainsi: {1, 2, 4, 8} en rouge et {3, 5, 6, 7} en bleu, on vérifie que la somme de deux nombres d'une même couleur n'est jamais de la même couleur. Le nombre cherché est donc au moins égal à 8. En revanche, comme $9=8+1=3+6$, il est illusoire de chercher à «prolonger» ce coloriage à [1, 9] sans avoir de nombres cotassés.
Et cette impossibilité est générale, quel que soit le coloriage en deux couleurs. Démontrons-le.
Prenons un coloriage quelconque des nombres de [1, 9] en deux couleurs. Parmi les cinq nombres {5, 6, 7, 8, 9}, au moins trois sont de la même couleur; appelons S cette couleur et a, b et c les trois nombres rangés ainsi: $5\leq a<b<c\leq 9$. Définissons aussi $b'=c-a$, $c'=b-a$ et $a'=c-$ b. On vérifie que b' et c' sont dans l'intervalle [1, 4] et on calcule $b'-c'=(c-a)-(b-a)=c-$b. Si b' est colorié en S alors b' et a sont cotassés. De même pour c'. Sinon, b' et c' ne sont pas coloriés en S et si $a'=b'-c'$ n'est pas, lui non plus, colorié en S alors c' et a' sont cotassés et sinon $a'=b-c$ est colorié en S donc a' et b sont cotassés. Conclusion: Quel que soit le coloriage, dans tous les cas, on a trouvé deux nombres cotassés. Le nombre maximum recherché doit donc être strictement plus petit que 9. Nous avons vu qu'il doit aussi être au moins égal à 8: c'est donc 8. Il s'agit du nombre de Schur faible $WS(2)$ décrits page 38.

Réponse 2: 55

Solution. Appelons R_n le nombre de randonnées allant de 1 à un entier n. La dernière étape avant d'atteindre n, peut être un ajout de 2 provenant de $n-2$ (il y en a R_{n-2}) ou bien un ajout de 1 provenant de $n-1$ (il y en a R_{n-1}) donc $R_n=R_{n-1}+R_{n-2}$. Comme $R_2=1$ et $R_3=2$, (R_n) est la suite de Fibonacci. Par conséquent, $R_1=F_{10}=55$. Le nombre de randonnées cherché est 55.

Réponse 3: 1, 2, 3, 6, 12, 24, 48, 96, 192 et 384

Solution. Voici une possibilité pour cette liste de dix entiers positifs. Commençons par les deux premiers entiers positifs, 1 et 2. Le nombre suivant sera $1+2=3$, le quatrième sera $1+2+3=6$, le cinquième sera $1+2+3+6=12$. Nous observons que par construction, la somme est maintenant toujours divisible par tous ses termes puisque chaque nouvel élément est le double du précédent.
Continuons ce procédé jusqu'à obtenir le dixième élément de la liste, qui sera 384. Ainsi 1, 2, 3, 6, 12, 24, 48, 96, 192, 384 est une liste recherchée, chaque élément divisant la somme totale, ici 768. D'une façon générale, pour construire une telle liste, il faut la commencer avec un nombre entier positif a et son double $2a$.

Réponse 4: $r=1$

Solution. Écrivons le nombre r sous la forme d'une fraction irréductible $r=a/b$: les nombres a et b sont alors deux entiers naturels premiers entre eux. On a alors $r+1/r=(a^2+b^2)/ab$. Si ce nombre est un entier, le dénominateur ab doit diviser le numérateur a^2+b^2. Ainsi, a divise a^2+b^2, donc il doit diviser b^2. Comme a et b sont premiers entre eux, cela entraîne $a=1$. De manière analogue, on montre que $b=1$. Cela entraîne $r=1$. Comme réciproquement 1 est clairement solution, on voit que $r=1$ est l'unique nombre rationnel positif répondant à la question.

Réponse 5: $(x, y)=(2, 5)$ et $(3, 7)$

Solution. Dès que $x\geq 5$, le dernier chiffre de $x!$ est un 0, donc le dernier chiffre de $x!+3$ est un 3 et celui de $6\times(x!+3)$ est un 8. Or, le dernier chiffre d'un nombre au carré comme y^2 est 0, 1, 4, 5, 6 ou 9, donc le dernier chiffre de y^2+5 est 0, 1, 4, 5, 6 ou 9, mais pas 8. Cela montre que le cas $x\geq 5$ est impossible. Il ne reste qu'à examiner les cas suivants.
Si $x=1$ alors $6\times(x!+3)$ vaut 24. Comme 19 n'est pas le carré d'un nombre entier, cela ne correspond pas à une solution.
Si $x=2$ alors $6\times(x!+3)$ vaut 30. Comme $25=5^2$, cela correspond à la solution $(x, y)=(2, 5)$.
Si $x=3$ alors $6\times(x!+3)$ vaut 54. Comme $49=7^2$, cela correspond à la solution $(x, y)=(3, 7)$.
Si $x=4$ alors $6\times(x!+3)$ vaut 162. Comme 157 n'est pas le carré d'un nombre entier, cela ne correspond pas à une solution.
Les seules solutions sont donc $(x, y)=(2, 5)$ et $(3, 7)$.

Réponse 6: 32916

Solution. La décomposition en facteurs premiers de 156 est $2^2\times 3\times 13$. Donc $32a1b$ doit être divisible par 4, par 3 et par 13. Pour que ce nombre soit divisible par 4, il faut que le nombre formé par ses deux derniers chiffres (en l'occurrence $1b$) soit divisible par 4. On en déduit $b=2$ ou $b=6$.
Si $b=2$, alors pour que le nombre soit divisible par 3, il faut que a soit égal à 1 ou 4 ou 7, car la somme des chiffres du nombre $32a12$ doit être divisible par 3. Cependant, aucun des nombres alors obtenus n'est divisible par 13.
Si $b=6$, alors pour que le nombre soit divisible par 3, il faut que a soit égal à 0 ou 3 ou 6 ou 9. On obtient alors les nombres: 32016, 32316, 32616 et 32916. Le seul divisible par 13 est 32916.

Réponse 7: 18.

Solution. Remarquons d'abord que l'ensemble de nombres cherché contient au maximum huit nombres, tous inférieurs ou égaux à 8. Pour que le produit de ces nombres soit le plus grand possible, il faut que ces nombres soient différents de 1. Ainsi les