

pendu son vol. On ne savait que faire des courbes elliptiques $E(A,B,C)$ que l'on pouvait associer à une hypothétique solution non triviale de l'équation de Fermat.

L'explosion de 1986 et le théorème de Wiles

On a dit que le coup de baguette magique fut donné en 1985 par G. Frey, alors professeur à l'Université de Sarrebruck. G. Frey conjecturait que nos courbes $E(A,B,C)$ devaient contredire la conjecture de Taniyama, et, merveille des merveilles, la communauté mathématique le crut ! Jean-Pierre Serre, d'ordinaire si prudent, tira le «coup de feu qui fit le tour du monde» en publiant de profondes conjectures dont découlait le théorème de Fermat. Peu de temps après, en 1987, B. Mazur et K. Ribet prouvèrent ces conjectures pour la représentation hypothétique du groupe de Galois absolu qui serait liée à une solution non triviale de l'équation de Fermat, mais à une condition : il fallait que la courbe $E(A,B,C)$ vérifie la conjecture de Taniyama.

Stimulé par le théorème de Ribet, le mathématicien britannique Andrew Wiles s'embarqua seul pour un long voyage sur des «océans étranges de pensée».

La navigation fut rude, et ce n'est qu'en 1991 que quelques oiseaux dans le ciel signalèrent la proximité d'une terre. En 1992, il pensait arriver près du but, et le 21 juin 1993, à l'Institut Newton, il annonça que le théorème de Fermat était démontré.

Las, l'annonce était prématurée, et les oiseaux disparurent de l'horizon. Un autre mathématicien aurait sans doute abandonné, mais A. Wiles n'écoula que son courage et son collègue R. Taylor ; celui-ci l'incitait à revenir sur sa route. C'est alors que, le 19 septembre 1994, il vit en un éclair la solution tant cherchée : un procédé découvert par Ehud de Shalit ouvrait un chemin plus direct vers la conjecture de Taniyama pour les courbes $E(A,B,C)$.

Un chef-d'œuvre est né et un mythe est mort : le théorème de Fermat est enfin démontré. De plus, le travail d'Andrew Wiles ouvre la voie à un vaste continent de recherches futures où de nombreuses conjectures restent à prouver.

Par ailleurs, la liste des équations diophantiennes abordables par la méthode des courbes $E(A,B,C)$ est loin

LES DIFFÉRENTES ROUTES EMPRUNTÉES DEPUIS FERMAT

LA ROUTE DES PIÉTONS

Cette route a été empruntée par Fermat lui-même pour l'exposant 4, puis par Lamé et Lebesgue pour l'exposant 7.

On se ramène à l'impossibilité de la résolution en nombres entiers des équations $t^2 = r^4 + 4s^4$ lorsque n est égal à 4, et $t^2 = r^4 - 3/4r^2s^2 + 1/7s^4$, lorsque n est égal à 7 (rst différent de zéro) et on procède par descente infinie.

LES FORMES QUADRATIQUES

On peut penser que, pour les exposants p premiers impairs, Fermat associait à son équation la forme quadratique $X^2 + (-1)^{(p+1)/2}pY^2$. C'est du moins ainsi que procédèrent Euler pour p égal à 3, puis Legendre et Dirichlet pour p égal à 5.

LES EXTENSIONS CYCLOTOMIQUES

Depuis De Moivre au XVIII^e siècle, on sait factoriser $x^p + y^p$ en produit de facteurs du premier degré en x et y , et cela conduit à considérer l'ensemble des nombres déduits par additions, soustractions et multiplications de $\zeta_p = e^{2\pi i/p}$, c'est-à-dire l'anneau des entiers cyclotomiques. C'est ainsi que Kummer parvint à démontrer l'assertion de Fermat pour tous les nombres premiers "réguliers". Malheureusement on ne sait pas démontrer qu'il existe une infinité de tels nombres.

L'APPROCHE ELLIPTIQUE

Elle est beaucoup plus récente que les précédentes (26 ans) et fait l'objet de cet article.

REMARQUES

- 1) Les trois premières méthodes font usage de la descente infinie pour prouver le second cas (défini dans l'article).
- 2) Une forme quadratique apparaît dans la route des piétons pour l'exposant 7.
- 3) Le nombre quadratique $((-1)^{(p-1)/2}p)^{1/2}$ apparaît implicitement dans la seconde méthode : il appartient à l'anneau des entiers cyclotomiques.
- 4) Finalement le corps des nombres cyclotomiques est contenu dans le corps engendré par les coordonnées des points de p -division de la courbe $E(A,B,C)$.

d'être close. Pourtant les solutions d'une équation aussi voisine du théorème classique, que $x^n + y^n = 2z^n$ ne peuvent être étudiées directement par cette méthode puisque cette équation possède la solution non triviale (1,1,1). Fermat n'est sans doute pas aussi mort qu'on le suppose, et sa note marginale suscitera peut-être d'autres découvertes.

À ce stade du panorama et après deux articles portant sur le sujet, le lecteur a une idée sur le comment du théorème de Fermat. Le pourquoi de ces recherches peut lui sembler énigmatique : il nous semble que cette question ne peut être examinée en termes logiques et que le pourquoi des mathématiques reste et restera un choix artistique. Le mathématicien Emil Artin exprime avec force ce point de vue : «Nous pensons tous que les mathématiques sont un art... Certes les mathématiques sont logiques : chaque conclusion est tirée des résultats qui précèdent. Cependant la totalité de l'affaire, l'œuvre d'art véritable, n'est pas linéaire ; et, ce qui est bien pire, sa

perception ne peut être qu'instantanée. Nous avons tous éprouvé, en de rares occasions, une impression d'exaltation en réalisant que nous avions permis à nos auditeurs de voir, l'espace d'une seconde, l'architecture complète d'une question, et toutes ses ramifications.»

Yves HELLEGOUARCH est professeur de mathématiques à l'Université de Caen.

Catherine GOLDSTEIN, *Un théorème de Fermat et ses lecteurs*, Presses Universitaires de Vincennes, 1995.

Grand théorème de Fermat, in *Quadrature*, n°22, été 95.

Séminaire Bourbaki, Exposés de Jean-Pierre Serre et Joseph Oesterlé. Juin 1995.

Yves HELLEGOUARCH, *Points d'ordre $2p^n$ sur les courbes elliptiques*, in *Acta Arithmetica* XXVI, 1975.

K.A. RIBET, *Galois Representations and Modular Forms*, in *Bulletin of the American Society*, Octobre 1995.

Partage de butin

IAN STEWART

Des protocoles de partage proportionnels, plaisants ou partiels.

Arthur Barberousse renversa le sac sur la table de la cuisine. Jo le Teigneux, Denis Tourtencuisse et Léon la Volette regardaient, émerveillés, les paquets de billets et les tas de bijoux qui en sortirent. Restait le plus difficile : diviser le butin. Personne n'avait confiance et chacun voulait avoir sa part, sans être lésé. La justice, c'est la justice, n'est-ce pas ?

Arthur partagea rapidement l'argent, en se fondant sur la valeur affichée. C'était facile : il suffisait de diviser la valeur totale en quatre. En revanche, le partage des bijoux était plus épineux, car chaque membre de la bande avait son idée sur la valeur des divers bijoux. Certains objets, telles les chaînes, pouvaient se couper en morceaux, ce qui facilitait le travail, mais les autres...

«Ne traînons pas, dit Jo. La police doit être sur nos traces, et tout cela doit disparaître rapidement.

— Je vais prendre cette tiare de diamants, dit Léon, en se la mettant sur la tête. Et Jo aura les colliers et le...

— Pas question, intervint Denis : des canailles de votre espèce ne seront jamais d'accord si elles procèdent ainsi. Il faut une méthode qui nous garantisse à chacun un partage équitable.

— Ouais, dit Léon.»

Silencieux, ils regardèrent le tas de bijoux. Trois heures après, ils le regardaient encore :

«Ce dont nous avons besoin, dit Denis, c'est de ce que les mathématiciens nomment un "protocole de partage proportionnel plaisant", PPPP en abrégé.

— Aïe, dit Arthur. Et c'est quoi, ce truc ?

— Plaisant, c'est lorsque personne n'a le sentiment que quelqu'un d'autre a obtenu quelque chose qu'il ne...

— Je comprends "plaisant", mais les longs mots d'avant ?

— Un "protocole de partage", c'est une méthode systématique pour partager les choses entre plusieurs personnes. Il est "proportionnel" si chaque personne est satisfaite d'avoir reçu au moins sa juste part, et si personne n'estime qu'un autre a eu plus que sa part.

— N'est-ce pas la même chose que plaisant, demanda Léon ?

— Pas du tout.

— Oui, ajouta Denis. Les protocoles plaisants sont toujours proportionnels, mais les protocoles proportionnels ne sont pas nécessairement plaisants.

— Pourquoi ?

— Par exemple, suppose que, tous les trois, vous partagiez trois objets, comme un bracelet, un collier et une paire de boucles d'oreilles, et que vous assigniez subjectivement des valeurs de la façon suivante :

	Bracelet	Collier	Boucles
Arthur	40	50	10
Léon	30	50	20
Jo	30	20	50

Le partage est proportionnel si Arthur reçoit le bracelet, si Léon a le collier et si Jo a les boucles, parce que chacun d'entre vous aura reçu plus de 33 pour cent de la valeur totale, mais Arthur ne trouvera pas plaisant que Léon ait le collier, qu'il estime valoir plus que le bracelet. Comme nous le verrons, les protocoles plaisants sont beaucoup plus difficiles à trouver que les protocoles proportionnels.

En plus du protocole, des stratégies personnelles garantissent à chacun qu'il atteigne son but. Ces stratégies ne font pas partie du protocole ; elles sont d'ailleurs souvent implicites, mais ce sont elles qui garantissent que le protocole est juste. On nomme souvent "joueurs" les personnes entre lesquelles s'effectue le partage, parce qu'on peut envisager ce dernier comme une suite de coups dans un jeu, et l'on peut aussi représenter les valeurs comme des parts d'un gâteau. On se partage le gâteau, quoi.

Pour deux joueurs, par exemple Arthur et Léon, il existe un PPPP simple, que j'appelle «je coupe, tu choisis» : Arthur coupe le gâteau en deux parts égales, et Léon choisit celle des deux parts qu'il préfère. Avec ce protocole, la stratégie d'Arthur doit être de couper des parts égales à son goût, de sorte qu'il ne puisse perdre, quel que soit le choix que fera Léon. Pour Léon, la stratégie doit être de choisir la part qui lui semble la plus grosse. La stratégie d'Arthur lui assure une part qu'il estime à 50 pour cent, et celle de Léon une part que Léon estime supérieur ou égale à 50 pour cent. Le protocole est bien un PPPP.»

Comme Denis semblait bien connaître le problème, les trois autres l'envoyèrent à la bibliothèque de l'université locale pour y dénicher des informations supplémentaires et authentifiées. Denis découvrit que les mathématiques des partages naquirent dans la Pologne en guerre, à Lvov : en 1944, alors que l'armée soviétique combattait pour reprendre la Pologne aux Allemands, le mathématicien Hugo Steinhaus chercha à se changer les idées en résolvant un problème de partage. Il connaissait le protocole "Je coupe, tu choisis" pour partager le gâteau entre deux personnes et les stratégies conduisant chacune d'elles à penser que sa part est au moins égale à la moitié. Avec cette technique, aucun des deux joueurs n'a de raison de se plaindre : celui qui coupe peut faire une découpe impartiale, et celui qui choisit décide ce qu'il veut prendre ; aucun des deux n'est forcé de faire un choix qu'il jugerait injuste.

«Steinhaus, dit Denis quand il revint vers ses trois acolytes, se demanda si on pouvait diviser un gâteau entre trois personnes.

— Voyons, dit Arthur. Peut-être pourrais-je couper le gâteau en trois parts que j'estimerai égales, puis faire choisir Léon et ensuite Jo ?

— Non, protesta Jo : je ne marche pas, car je choisirais ainsi après Léon, et je risquerais d'avoir une part moins grosse que la sienne.»

Denis expliqua alors que Steinhaus avait abouti à une suite de neuf étapes à l'issue de laquelle chaque joueur est satisfait, car il a ce qu'il considère être au moins un tiers du gâteau. Afin d'examiner ce protocole proportionnel, procédons à quelques définitions. Un joueur estime qu'une part est «juste» si la taille de cette part lui semble au moins égale à un tiers ; sinon elle est «injuste». «Passer», à une certaine étape du protocole, c'est ne rien faire. Par commodité, nous parlerons de «taille des parts», mais il s'agit de valeur relative, estimée par un joueur. Tous les jugements sont subjectifs et propres au joueur qui a le trait. Les indications entre parenthèses ne font pas partie du protocole ; ce sont des commentaires sur les stratégies utilisées par les joueurs.

Voici maintenant le protocole de Steinhaus (voir la figure 1) :

1. Arthur coupe le gâteau en trois parts (qu'il juge toutes justes, c'est-à-dire subjectivement égales).

2. Léon peut : soit passer (s'il pense qu'au moins deux parts sont justes) ; soit étiqueter deux parts (qu'il juge injustes) comme «mauvaises».

3. Si Léon passe, Jo choisit une part (qu'il estime juste). Puis Léon choisit une part (qu'il estime juste) et, finalement, Arthur prend la dernière part.