Année 2000 : présentation des prix du Millenium par le Clay Institute (exposant : John Tate [1])

Andrew Wiles : Nous allons maintenant entendre les conférences sur les problèmes du prix du Millénaire. Ces problèmes ne sont pas nouveaux ; ils ont été sélectionnés par l'Institut mathématique Clay car ils constituent de grands problèmes non résolus du XXe siècle. Ce sont des problèmes qui, nous en sommes convaincus, doivent un jour être résolus (*petite ambiguité en langue française : au sens de "ils seront résolus un jour"*). Ce sont des problèmes que nous pensons faciles à énoncer et à expliquer. Ce sont des problèmes qui, nous en sommes convaincus, ouvriront des perspectives mathématiques entièrement nouvelles, des perspectives que nous ne pouvons même pas imaginer à l'heure actuelle. Les trois premiers problèmes du prix du Millénaire seront présentés par le professeur John Tate. Le professeur Tate est titulaire de la chaire Sid Richardson à l'Université du Texas à Austin et a été auparavant professeur Perkins à l'Université de Harvard. Sa longue et brillante carrière coïncide avec la grande reformulation de l'arithmétique et de la géométrie qui a eu lieu depuis les années 1950 et il a contribué à façonner cette reformulation. Une grande partie des débuts de cette révolution s'est déroulée ici, à Paris. Le professeur Tate lui-même entretient des liens étroits avec les institutions parisiennes et, parmi ses nombreuses distinctions, il est membre associé de l'Académie des sciences française. De plus, je sais que certains de ses grands théorèmes ont été démontrés pendant son séjour à Paris. Il a été une grande source d'inspiration pour moi, en tant qu'étudiant. Et en tant que jeune professeur, comme il l'a été pour beaucoup d'autres de ma génération et de celles qui m'ont précédé et suivi, c'est un grand plaisir pour moi d'inviter le professeur Tate à décrire les trois premiers problèmes du prix du Millénaire.

John Tate : Merci Andrew.

En mathématiques, le premier problème a une longue histoire et je m'excuse auprès des experts, je vais être aussi historique et élémentaire que possible dans la description des problèmes. Alors, commençons avec la suite des nombres premiers. Euclide savait déjà que tout nombre peut être exprimé comme un produit de nombres premiers, tout nombre supérieur à un, comme vous le voyez ici. Il a utilisé ce fait pour prouver que la suite des nombres premiers ne s'arrête jamais. Si elle s'arrêtait, s'il n'y avait qu'un nombre fini de nombres premiers, on pourrait les multiplier et ajouter un, et on obtiendrait un nombre supérieur à tous les nombres premiers de l'ensemble fini, et qui n'est divisible par aucun nombre premier de cette ensemble, à cause du +1. Cela contredirait le fait que tout nombre est un produit de nombres premiers. Euclide n'a jamais affirmé que la factorisation d'un nombre en nombres premiers ne pouvait se faire que d'une seule manière, c'est ce qu'on appelle la factorisation unique, le théorème fondamental de l'arithmétique. Mais il a énoncé un lemme dont découle ce théorème. Voici une conséquence simple de ce lemme, qui illustre la notion de primalité, à savoir que si un nombre premier p divise le produit de deux nombres, alors p divise l'un ou l'autre de ces deux nombres. Aux alentours de 1700, on observe un grand saut autour de 1750. Considérons une fonction, maintenant appelée $\zeta(s)$, définie par ce produit sur les nombres premiers. L'égalité a lieu entre le produit calculé sur les nombres premiers et la somme calculée sur les nombres entiers naturels.

1. https://www.youtube.com/watch?v=QBcnsrInG3g.
Révision de la traduction ia : Denise Vella-Chemla, octobre 2026.

Ceci est une expression analytique de l'idée d'unicité de la factorisation. La démonstration de cette égalité, valable lorsque ces produit et somme convergent (c'est-à-dire pour $s > 1$), consiste simplement à développer ce produit, et à remarquer que chaque terme du développement du produit en somme est obtenu en choisissant un terme dans chaque facteur pour chaque nombre premier, et bien sûr on a ainsi un terme pour tout nombre fini. Ainsi, puisque chaque nombre est un produit unique de nombres premiers, cette égalité est vraie. Cette égalité est la formulation analytique de l'unicité de la factorisation. Euler a légèrement amélioré la preuve de l'infinité des nombres premiers d'Euclide. Comme tout bon étudiant en calcul différentiel et intégral le sait, le critère de comparaison montre que la somme des inverses des nombres est infinie. En prenant les logarithmes et en utilisant cette égalité, on constate que la somme des inverses des nombres premiers est également infinie, bien que cette somme tende vers l'infini très lentement. Pour des nombres premiers supérieurs à trois ou quatre, il faut considérer des nombres premiers de plusieurs millions. Euler est également devenu célèbre en évaluant la fonction ζ pour $x = 2$, c'est-à-dire en sommant la série des inverses des carrés. Si l'on souhaite approfondir la distribution des nombres premiers, il faut adopter une approche plus quantitative et introduire la fonction suivante : $\pi(x)$, qui représente le nombre de nombres premiers inférieurs à x. Par exemple, $\pi(10) = 4\pi$, et $\pi(100\,000\,000) = 5\,761\,455$. Si je ne me trompe pas, euh, d'accord, alors combien y a-t-il de nombres premiers inférieurs à environ 1800 ? Par expérimentation, j'ai estimé que la probabilité qu'un nombre premier proche de x soit premier est $\dfrac{1}{\log x}$, ou de manière équivalente, que $\pi(x)$ est très bien approché par le logarithme intégral de x, qui est défini ici [2]. En effet, si vous tracez un graphique sur lequel x tend vers 100 000 et $\pi(x)$ en fonction de x, alors, à une très fine ligne de crayon près, ces deux fonctions coïncident. Cinquante ans plus tard, Chebychef a introduit une modification de la fonction $\pi(x)$, techniquement meilleure, et a prouvé une relation entre ce $\pi(\pi(x))$ et la fonction ζ de Euler, appelée maintenant fonction ζ de Riemann, qui s'écrit ainsi. C'est le thème de ce problème du millénaire sur l'hypothèse de Riemann : la relation entre la distribution des nombres premiers et la fonction zêta. Chebychef a également montré que s'il existait une approximation raisonnable de $\pi(x)$, alors, dans un certain sens, L'approximation devait être l'intégrale logarithmique, puis une grande percée a eu lieu et j'ai décidé de commencer à utiliser la couleur. Environ 10 ans plus tard, Riemann a inversé l'hypothèse et a pu démontrer que la fonction zêta avait un sens pour tous les nombres complexes différents de 1, où elle possède un pôle, et qu'elle satisfait effectivement une équation fonctionnelle reliant $\zeta(1 - s)$ à $\zeta(s)$. Il a pu, en utilisant l'argument complexe, l'analyse de Fourier, la transformée de Fourier et en évaluant une intégrale en sommant les résidus aux singularités de $\log \zeta$, prouver que $\pi(x)$, qui donne la distribution exponentielle des nombres premiers, est le logarithme intégral moins la somme des valeurs de $\mathrm{Li}(x)$ aux endroits où la fonction zêta est nulle. Le premier problème du prix Clay, le problème du millénaire, est la célèbre hypothèse de Riemann, qui consiste à prouver que si r est un nombre complexe tel que $\zeta(r) = 0$ et n'est pas l'un des zéros triviaux (pour les entiers négatifs pairs, la fonction ζ s'annule trivialement), alors, la partie réelle des zéros non triviaux, donc, est égale à $1/2$. Autrement dit, en dessinant les nombres complexes ici, avec 0 ici, 1 ici et -1 là, les zéros triviaux sont ici : $-2, -4, -6$. Tous les autres zéros devraient se trouver sur cette droite, appelée la droite critique, et qui est la droite des nombres complexes de partie réelle $1/2$. Riemann lui-même a calculé les premiers zéros, le premier étant aux alentours de 14. Il a estimé le nombre de zéros jusqu'à un certain point et a dit qu'ils semblaient tous être sur la

2. $\mathrm{Li}(x) = \displaystyle\int_0^x \frac{\mathrm{d}t}{\ln \mathrm{d}t}$.

droite critique, mais après quelques tentatives rapides de démontrer cela, il a abandonné. C'était vers 1860. Cette démonstration n'était pas nécessaire à Riemann pour atteindre son objectif immédiat, qui, je tiens à le souligner, était de relier et de donner une formule pour la distribution des nombres premiers en fonction des zéros de la fonction zêta (la fameuse formule explicite), eh bien, c'était il y a 140 ans. Celui qui résoudra ce problème aura mérité sa récompense. De nombreux grands esprits mathématiques ont réfléchi à ce problème et n'ont pas réussi à le résoudre. D'un autre côté, il y a toutes les raisons de croire que l'hypothèse de Riemann est vrai. Euh, au moins, il existe de nombreuses preuves numériques que les 1,5 milliard de premiers zéros de la fonction ζ se situent sur la droite critique, et leur partie réelle monte jusqu'à une hauteur d'environ 500 millions (calculés par Andrew Odlyzko). Il y a des raisons de penser que si un zéro est hors de la droite critique, il pourrait se situer un peu plus haut, dans divers intervalles, une hypothèse a été émise à ce sujet, et Andrew Odlyzko a vérifié que dans tous les intervalles jusqu'à une hauteur de 10^{20}, tous les zéros de ces intervalles sont sur la droite critique, ce qui représente environ 10 100 millions de zéros au total. Théoriquement, on sait qu'environ 40 % des zéros sont sur la droite critique, ce qui ne semble pas idéal. Mais cela est prouvé. J'ai omis de mentionner que le problème consistant à montrer que ces zéros sont sur la droite critique est équivalent à montrer que $\mathrm{Li}(x)$ est la meilleure approximation possible de $\pi(x)$, c'est-à-dire que l'erreur est de l'ordre de la racine carrée de $x \log x$, et il est théoriquement connu qu'on ne peut pas faire beaucoup mieux.

L'idée est que si l'on pouvait prouver que tous les zéros, par exemple, se situaient à gauche de la droite 3/4 (i.e. des nombres complexes qui ont une partie réelle égale à 3/4), on obtiendrait $3x^{3/4} \log x$. Personne ne peut le faire pour l'instant pour un nombre inférieur à un [3], et les meilleures erreurs dans l'estimation de $\pi(x)$ par $\mathrm{Li}(x)$ sont obtenues en trouvant des régions sans zéros, mais celles-ci s'estompent et deviennent très fines lorsqu'on s'éloigne de x [4]. Cependant, la principale raison de croire en cette hypothèse de Riemann, selon laquelle les zéros sont sur la droite, est liée à des cas analogues où elle a été prouvée et est très complexe. La fonction zêta est un prototype d'un type général de fonction appelée fonction L définie par un produit d'Euler. Je ne l'ai pas dit, mais ce produit sur les nombres premiers, et les produits similaires, sont appelés produits eulérien, d'après Euler, les fonctions L sont définies par un produit d'Euler dans un demi-plan droit et on s'attend à ce que ces fonctions L satisfassent une équation fonctionnelle. Je ne peux pas définir la plus générale, mais j'ai une suggestion : pour tout anneau intègre de type fini, on obtient une fonction de ce type L, généralisant la fonction zêta résiduelle, simplement en remplaçant le produit sur les nombres premiers qui engendrent les idéaux maximaux de l'anneau des entiers par un produit sur le nombre d'éléments des corps résiduels des idéaux maximaux de cet anneau intègre. Ainsi, si l'anneau intègre est l'anneau des entiers, souvent noté $\mathbb{Z}$ (d'après Bourbaki), on retrouve la fonction zêta résiduelle. Mais pour tout anneau, on obtient une fonction L, et il est conjecturé que les zéros et les pôles d'une telle fonction L se trouvent sur la droite dont la partie réelle est égale à un entier ou à un demi-entier.

Ceci est vrai si l'anneau intègre est de caractéristique supérieure à zéro, c'est-à-dire si l'addition de multiples nombres 1 finit par donner 0. C'est une longue histoire que je ne détaillerai pas ici, mais pour des anneaux unidimensionnels particuliers de ce type, Emil Artin a suggéré que cela devrait être vrai dans sa thèse. Helmut Hasse l'a démontré dans le cas des courbes de genre 1. Les courbes

3. Le nombre 3/4 en l'occurrence.
4. ?

de genre arbitraire ont suggéré une histoire très intéressante qui devrait être vraie pour les anneaux de dimensions supérieures et qui a été prouvée par Deligne dans les célèbres conjectures de Weil au début des années 70. Enfin, permettez-moi de mentionner l'hypothèse de Riemann étendue, qui stipule que lorsqu'on remplace $\mathbb{Z}$ par un anneau R d'entiers dans un corps de nombres algébriques, cette fonction zêta de R satisfait une hypothèse de Riemann pour tout corps de nombres. C'est l'hypothèse de Riemann étendue, et sa vérité impliquerait toutes sortes de choses que je n'ai pas le temps d'aborder maintenant. Le problème suivant que je veux aborder concerne également ces fonctions zêta généralisées, ou théorie des fonctions L. Mais j'ai entendu dire qu'il est d'usage de changer fréquemment de sujet pour ne pas ennuyer l'auditoire. Nous allons donc aborder les équations diophantiennes. La plus simple est $f(x) = 0$, où $f(x)$ est un polynôme dont les éléments sont des nombres rationnels. Les coefficients, étant irréductibles, ne peuvent être factorisés, même en autorisant des nombres complexes. Si l'on considère les solutions réelles de cette équation, on obtient une courbe. Si l'on considère les solutions complexes et que l'on supprime les points problématiques (là où la courbe se croise ou présente un point anguleux), on obtient une surface qui ressemble à la surface d'un tore avec plusieurs trous. Le nombre de trous est alors appelé le genre de cette courbe ; c'est l'invariant fondamental, le plus profond, le plus intrinsèque et essentiel de la courbe. Si l'on cherche des solutions en nombres rationnels, on se heurte à un problème majeur : soit il peut n'y avoir aucune solution, soit il peut y en avoir une infinité, et elles seraient dispersées le long de cette courbe de manière discrète.

On ne peut pas utiliser de simples méthodes d'observation géométrique pour comprendre ce qui se passe. Mais que se passe-t-il réellement ? C'est ce que Timothy Gowers a expliqué à propos de l'unité des mathématiques. Un exemple remarquable est la manière dont la représentation géométrique illustre la complexité des solutions et le nombre de trous influence le comportement des solutions sous forme de nombres rationnels, ce qui relève d'un problème arithmétique et discret. En l'absence de trous, tout est connu : lorsqu'il existe un point, on peut le paramétrer par projection. Cela a été fait pour le cercle il y a longtemps. L'existence d'un point peut être déterminée en vérifiant si les congruences correspondantes sont satisfaites. La congruence est satisfaite lorsque $g = 2$. Donc, pour $g = 2$, il n'y a pas de problème. Pour $g \geq 2$, il y a une trichotomie. Pour $g \geq 1$, il y a une dichotomie. Pour les genres supérieurs, Mordell a conjecturé en 1921 qu'il n'y aurait qu'un nombre fini de solutions rationnelles à toute équation de ce type, ce qui a été prouvé par Faltings en 1983. Il s'agit d'un développement extrêmement important. De nombreuses questions subsistent pour les genres supérieurs, notamment le nombre de points, etc. Mais ces dernières années, à l'exception des résultats de Faltings, la recherche s'est concentrée sur l'existence d'un point rationnel pour le genre 1. Il existe une méthode pour déterminer, pour une équation donnée, s'il existe un point, et cette méthode fonctionne en pratique. Cependant, personne ne peut prouver qu'elle aboutira toujours à une conclusion en un nombre fini d'étapes. S'il existe un point, alors après un changement de coordonnées (qui n'affecte pas vraiment le problème), on peut supposer que l'équation est sous forme cubique, comme ceci. Et maintenant… je suis vraiment maladroit, il me faut un crayon. Vous avez un crayon ? Merci. Eh bien, est-ce que cela fonctionnera ? Vous en avez un ? Oui, super. Puisque l'équation est cubique, et que toutes les cubiques sans point sont de genre 1, on peut faire beaucoup de choses. Si vous avez deux points, vous pouvez les relier par une ligne, et elle rencontrera la courbe en un troisième point. C'était déjà connu de Diophante. De plus, si vous prenez un point et que vous tracez la tangente en ce point, elle rencontre la courbe deux fois. Donc, elle la rencontrera une fois de plus. Diophante a utilisé cette idée pour poser

des problèmes complexes. Il s'agissait de trouver des points très compliqués avec des numérateurs et des dénominateurs très grands, en commençant par un point avec un petit dénominateur. En élevant approximativement le numérateur et le dénominateur à la puissance quatre, on obtient de très grands points à partir de petits. Fermat a utilisé la même idée dans l'autre sens, on parle alors de descente de Fermat au lieu d'ascension, parfois pour démontrer l'absence de solution ou la présence d'une solution triviale, en dehors des solutions évidentes. En 1921, Mordell a utilisé la même démonstration par descente en général pour montrer que sur une courbe de genre un, il existe toujours un ensemble fini de points. On peut donc partir de ces points, tracer des lignes, puis continuer en tangentes et ainsi de suite, jusqu'à trouver tous les points rationnels, ce qu'on appelle la génération finie. On peut ensuite organiser ces points en un groupe, et, d'après la théorie des groupes, ce groupe est isomorphe au produit direct des copies des entiers dans un groupe fini.

Ceci découle du résultat de Mordell, qu'il a démontré, et que R possède une invariance appelée rang. En résumé, cela signifie qu'il existe des points qui ne sont reliés par aucune méthode de tracé de lignes, mais le fait que tout rang $r + 1$ aura la propriété qu'elles sont si connectées qu'on peut passer de l'une à l'autre en traçant des lignes, c'est une propriété du rang. C'est une approximation grossière. Personne ne sait s'il existe des courbes elliptiques de rang arbitrairement élevé, et c'est un sujet qui a longtemps été un mystère. Mais on a appris... enfin, on a essayé de construire de telles courbes avec des rangs de plus en plus élevés. Ceci est une simple digression. Le record du monde, je crois, est de 24, du moins c'était récemment... Je suppose que vous ne pouvez pas lire ça, mais l'équation... Les entiers a et b dans l'équation ont 40 ou 50 chiffres, et voici les 24 points indépendants. Cela a été fait par deux personnes de la NSA aux États-Unis et ça a été classifié pendant un certain temps, à tort. Mais les courbes elliptiques se sont révélées utiles en cryptographie, et quelqu'un a classifié cela, et ce n'est que récemment que ces connaissances ont été déclassifiées. Bon, maintenant, parlons des fonctions L. À chaque courbe elliptique de ce type correspond une fonction L qui... Je vous ai montré le produit d'Euler, mais l'essentiel est que la fonction L dépend uniquement du nombre de solutions pour chaque nombre premier p de la congruence correspondante. a et b, j'ai oublié de le préciser, étaient des entiers dans l'équation, ce qui permettait de l'obtenir par un changement de variables. Cette fonction L, ce produit, a un sens pour une partie réelle de s supérieure à trois, mais on conjecture, ou plutôt on conjecturait, qu'elle a un sens pour tous les nombres complexes.

Définissons ensuite le rang analytique. Il n'a rien à voir avec les zéros de la fonction zêta (je m'excuse d'utiliser la même lettre). Le rang analytique est l'ordre du zéro de cette fonction en $s = 1$. Cette fonction a un développement en série linéaire d'une constante non nulle (temps constant $s - 1$) à la puissance le rang analytique en question, plus les termes d'ordre supérieur. Bien que la série ne converge pas, cela a du sens grâce à Andrew Wiles et au groupe de personnes qui ont complété son travail démontrant que toute courbe elliptique est modulaire, car cela est plus ou moins équivalent au fait que cette série L l'est aussi. Cela implique que cette série L est cohérente partout et possède une équation fonctionnelle reliant s et $2 - s$.

Le second problème que je souhaite aborder est de démontrer que ce rang analytique est égal au rang algébrique R du groupe des points rationnels. C'est la conjecture de Birch-Swinnerton-Dyer, formulée vers 1960. Ils ont été amenés à cette idée, ou du moins encouragés (je ne connais pas précisément l'historique), en remplaçant s par 1 dans cette équation. Il n'est pas pertinent de considérer

le produit infini, mais on peut utiliser les produits partiels, notés p/n_p, où n_p est le nombre de solutions de la congruence. L'idée est que plus le rang est élevé, plus il y a de points rationnels, donc plus il y a de solutions, plus n_p est grand et plus ce produit est petit. Voilà l'idée. Il existe également une conjecture plus forte qui exprime cette conjecture en termes d'invariance de la courbe, du groupe de Shafarevich, du déterminant de hauteur, du carré de la torsion et de la constante, qui est le produit des termes locaux. Je n'entrerai pas dans les détails, donc vous pourriez appeler ceci la conjecture faible et ceci la conjecture forte.

Pourquoi croyons-nous à ces conjectures ? Eh bien, les séries de Birch-Swinnerton-Dyer elles-mêmes ont fourni de nombreux cas numériques spécifiques, dont le cas particulier de la conjecture qui dit que si la série L ne s'annule pas lorsque $s = 1$, alors le rang est nul. En d'autres termes,on considère que cette manière d'utiliser les points est finie, mais la meilleure preuve, à mon avis, comme pour l'hypothèse de Riemann, se trouve dans le cas des corps de fonctions, c'est-à-dire lorsqu'on a affaire à des anneaux de caractéristique supérieure à zéro. Shafarevich et moi avons pu démontrer que le rang analytique dominant est toujours supérieur ou égal au rang algébrique, et que la conjecture faible est équivalente à la conjecture forte. Dans un certain cas de la caractéristique (se reporter à la partie qui concerne les caractéristiques), il en découle que la conjecture est vraie lorsque le rang analytique est nul, lorsque la fonction L ne s'annule pas. Que se passe-t-il alors sur les corps de nombres rationnels ? La première grande avancée a été due à Coats et Wiles, qui ont prouvé que sur les rationnels, si la courbe admet une multiplication complexe, la conjecture était vraie lorsque le rang analytique était nul. Gross et Zagier, utilisant une ancienne idée de Hegner, ont ensuite obtenu une version beaucoup plus aboutie dans un direction impressionnante, à savoir qu'il s'agit de l'inégalité triviale, c'est-à-dire l'inégalité la plus simple, ou philosophiquement la plus simple. L'autre inégalité produirait un rang élevé, c'est-à-dire des points sur la courbe, des points rationnels, ce qui est plus difficile, mais Gross et Zagier ont produit des points de Hegner lorsque le rang analytique était de un. Puis, quelques années plus tard, c'était au début des années 1980, je crois, et quelques années plus tard, un mathématicien a prouvé que la conjecture est vraie lorsque le rang est de zéro ou un. Ces mathématiciens ont pu prouver une partie de la conjecture plus forte, mais on n'a pas la moindre idée de ce qu'il faut faire lorsque R est supérieur ou égal à deux, lorsque le rang analytique est de 0 ou 1, lorsque la fonction L s'annule deux fois. Il est intéressant de noter que les rangs égaux à 0 et 1 sont précisément les cas où il est facile de décider, en calculant précisément la fonction L, si le rang est de un ou non, en raison de l'équation fonctionnelle. On peut faire une vaste généralisation de cette conjecture si vous vous souvenez de la fonction zêta associée à un domaine intègre arbitraire. J'ai mentionné R précédemment. On peut dire que si l'on considère le point où la dimension de R est égale à 1, l'ordre de cette fonction devrait être le rang des unités dans R moins le rang du groupe des classes de diviseurs de R. Dans le cas où R est cet anneau, cela signifierait que c'est la même chose que la conjecture de Birch-Swinnerton-Dyer. Mais c'est évidemment beaucoup plus général. La conjecture de Birch-Swinnerton-Dyer est un élément-clé dans le domaine des valeurs dites spéciales. Elle permet d'interpréter l'ordre d'annulation ou l'ordre d'un pôle d'une fonction L en un point entier et de relier le coefficient dominant du développement à l'invariance algébrique, comme le groupe de Shafarevich, etc. La première situation vraiment mystérieuse était celle de la conjecture de Birch-Swinnerton-Dyer.

Passons au troisième problème que je veux aborder, qui concerne la logique et l'informatique. Prenons un exemple : n et k sont des entiers, et une tâche pourrait consister à déterminer si n est un

entier parfait. Un autre problème pourrait être de déterminer si n est composé et factorisable. Un autre serait, étant donné n et k, de savoir si k divise n, ou si n est divisible par un nombre a compris entre 2 et k. Un autre problème encore pourrait être de trouver un diviseur premier de n. Un autre problème, que je n'ai pas besoin d'aborder grâce à Timothy Growers, consiste à colorier un graphe étant donné sa simplicité : "Pouvez-vous le colorier en trois couleurs ?". Il existe de nombreux autres problèmes, comme la somme des sous-ensembles, le problème du voyageur de commerce, et d'autres types de problèmes mathématiques. Par exemple, existe-t-il une courbe elliptique de rang supérieur ou égal à n ? Tous ces problèmes, sauf un, sont des problèmes de décision : "existe-t-il une courbe elliptique de rang supérieur ou égal à n ?". Ici, la recherche d'un nombre premier est un problème de recherche, mais on peut souvent réduire un problème de recherche à un problème de décision. Par exemple, ces deux problèmes sont équivalents car, en jouant au jeu des 20 questions, ou à la recherche dichotomique, si vous savez si vous pouvez déterminer si n possède un diviseur dans un intervalle donné, vous pouvez résoudre cet autre problème. Il n'est pas difficile de voir que vous pouvez cibler un diviseur premier ou un diviseur quelconque, puis refaire de même avec le diviseur quelconque. Logiquement, c'est un peu étrange, mais un problème de décision n'est rien d'autre qu'une liste L de nombres, comme les carrés parfaits, les nombres composés, etc. La tâche consiste simplement à déterminer si un nombre donné figure dans la liste. L signifie "liste" ici, mais il est plus courant de parler de langage. On remplace les chiffres de 0 à 9 par des lettres appartenant à un ensemble fini. Au lieu d'une suite de chiffres, on a une suite de lettres, que l'on appelle un mot. Un langage est donc constitué d'une liste de mots, généralement une liste infinie, donc un dictionnaire de tous les mots du langage. L peut donc être une liste de nombres ou un langage ; c'est logiquement équivalent. Voilà ce qu'est devenu la tâche. Un type de tâche correspond à un certain type de langage L. On dit que cette tâche est de type P si, comme l'a expliqué Timothy Gowers, on peut programmer un ordinateur qui sera capable d'exécuter la tâche en temps polynomial, c'est-à-dire si l'on peut programmer un ordinateur pour déterminer rapidement si un nombre donné, par exemple, figure dans la liste de nombres. Le temps nécessaire à la machine pour prendre sa décision est au plus une constante multipliée par une puissance de la longueur du nombre (c'est-à-dire le nombre de chiffres). Autrement dit, c'est un polynôme. Il est inférieur ou égal à un polynôme en la longueur du nombre, ou au logarithme du nombre si l'on utilise des mots, la longueur du mot. Pour comprendre cela mathématiquement, il faut définir ce qu'est un ordinateur. Dans le cas du problème de l'institut Clay, l'ordinateur est une machine à écrire. Mais peu importe, un grand nombre de processeurs parallèles avec des mémoires infinies peuvent résoudre ce problème avec un polynôme de degré inférieur à celui d'une machine à écrire, qui est un système très primitif avec une bande et un programme qui déplace une tête de lecture sur une bande, programme qui lit le caractère pointé par sa tête de lecture, et qui imprime des carrés sur la bande et qui est facilement descriptible mathématiquement. Mais qu'il s'agisse d'un problème, d'une liste ou d'un problème, le type de P n'a pas d'importance. Il existe une large gamme de possibilités, mais on peut aussi penser à d'autres types de machines, comme les ordinateurs quantiques, qui peuvent effectuer des tâches plus rapidement. L'expérience dont Timothy Gowers a parlé, ou plutôt la croyance en informatique, c'est qu'un problème de type P, résoluble en temps polynomial (polynomial par rapport à la longueur de l'entrée), est un problème pratiquement résoluble. Revenons à mes exemples (que j'ai égarés, où sont-ils ?). Lesquels de ces problèmes sont résolubles en temps polynomial ? Le premier l'est certainement : il ne faut pas longtemps pour déterminer si un entier est un carré parfait (c'est un problème de type P), miraculeusement si l'hypothèse de Riemann étendue est vraie. Le deuxième est également de type P, un résultat de Miller. Le troisième, en fait, consiste à factoriser un nombre,

non seulement en connaissant sa composition, mais aussi en trouvant ses facteurs. Cela n'est probablement pas polynomial, et c'est équivalent à la factorisation. C'est un problème de type A1. Les autres ne sont probablement pas des problèmes de type P. Bon, il faut se dépêcher. Non, oui. Eh bien, comme je ne connais pas grand-chose à ce problème, alors... Il y a A1. Il existe un autre type de problème appelé NP. Cela ne signifie pas "non polynomial". La notation NP est historique ; elle signifie "temps polynomial sur une machine non déterministe". Cela équivaut au problème suivant : si un être omniscient peut non seulement vous dire si un nombre donné figure sur la liste (est-ce un carré, un nombre composé, etc.), mais peut aussi vous fournir des preuves vous permettant de vérifier vous-même qu'il y figure, alors... Le problème de la factorisation d'un nombre est évidemment NP, car l'être omniscient peut vous donner la factorisation et vous pouvez la vérifier facilement en temps polynomial. Le problème de coloration des graphes planaires est connu pour être NP. Si l'on vous donne une coloration, vous pouvez vérifier en temps polynomial qu'aucun sommet adjacent n'est de la même couleur que tous ses voisins. Ces problèmes sont également NP. Existe-t-il une courbe elliptique de rang supérieur ou égal à n ? Qui sait ? Si quelqu'un prouve le théorème selon lequel il existe des courbes elliptiques de rang arbitrairement élevé, alors ce problème sera de type P. Mais je ne pense pas qu'il soit de type NP sans une telle preuve. Le troisième problème est une question étrange pour quelqu'un qui ne travaille pas dans ce domaine. Est-ce que P est égal à NP ? Bien sûr, tout problème résoluble en temps polynomial peut être vérifié en temps polynomial si la réponse est donnée. Donc, si p est un problème P, alors p est un problème NP. Mais la réciproque est-elle vraie ? Je pense que l'avis des experts est que non. La question est de savoir s'il existe des problèmes difficiles pour lesquels une réponse positive est facile à vérifier, ou inversement. Si, dans un problème de ce type, il existe une liste où l'on peut facilement vérifier qu'un nombre y figure, cela signifie-t-il que le problème est facile ? Quelle est l'histoire de ce problème ? Elle ne remonte pas aussi loin que les autres problèmes du millénaire, mais dans les années 1930, les logiciens Kurt Gödel et Alonzo Church, lors d'une conférence d'informaticiens, ont discuté de la décidabilité de leurs problèmes. Il s'agit d'un problème de logique pure, sans intérêt pour l'informatique, car le temps de résolution ne les intéressait pas. Au fait, le temps de résolution correspond au nombre d'étapes, proportionnel au nombre d'opérations sur l'ordinateur. Ils se demandaient simplement si on pourrait programmer une machine qui finirait par prendre une décision, quelle que soit la durée, par exemple en temps exponentiel, voire en temps doublement exponentiel. Il y avait ensuite la semi-décidabilité : si le nombre figure sur votre liste, l'ordinateur s'arrête et vous le signale ; sinon, il peut continuer indéfiniment. L'idée de temps polynomial a été mentionnée par Feymann dans les années 1950, puis approfondie par Edwards dans les années 1960. En 1970, Steven Cook a introduit le concept de NP-complétude, analogue à la semi-décidabilité. Une liste L est NP-complète si toute liste NP L' peut être réduite à une tâche de la liste L des problèmes NP-complets en temps polynomial. Autrement dit, c'est un problème dont la solution permet de résoudre tout autre problème NP. Dans les exemples, le problème du graphe, le problème de la somme des sous-ensembles et le problème du voyageur de commerce sont NP-complets. Pour montrer que P est égal à NP, il suffit de démontrer qu'une tâche NP-complète, par exemple choisir la couleur d'un graphe parmi trois, peut être réduite à une tâche de la liste L en temps polynomial. Si vous pouviez écrire un programme pour effectuer cette tâche en temps polynomial, alors P serait égal à NP. Sinon, pour remporter le prix, vous devez démontrer l'existence d'un problème NP, par exemple le problème du graphe, qu'il est impossible de programmer en temps polynomial. Chaque solution présenterait des avantages. Si vous pouviez prouver que P est NP, vous disposeriez d'un programme très efficace pour des tâches potentiellement utiles. En revanche, cela signifierait probablement que les

systèmes de chiffrement à clé publique actuellement utilisés, comme la factorisation RSA, ne seraient plus sécurisés. Ce sont les trois premiers problèmes du millénaire que je devais vous présenter.

Je vous remercie de votre attention.