Entretien avec Jean-Jacques Szczeciniarz

Alors qu'est-ce que vous voulez savoir ?

Et bien, du coup, le 4CT vous n'êtes pas trop compétent dessus ?

Si j'avais travaillé dessus, mais il y a au moins 15 ans, et puis il y a eu quelques articles mais je ne suis plus au fait de la démonstration, en revanche je connais d'autres formes de preuves par les preuves informatiques. Là, ça dépend de quel point de vue vous voulez qu'on prenne, parce qu'il y a en mathématiques ce qu'on appelle des preuves monstrueuses qui sont les preuves que l'esprit humain ne peut pas cerner et que la machine est capable de cerner pour toutes sortes de raisons : à cause d'une part de la longueur des calculs, d'autre part de la complexité des calculs. Et puis il se trouve, c'est une autre raison, qu'il y a en mathématiques, de plus en plus, des conjectures qui demandent ce type d'intervention. Il y a des conjectures célèbres, il y a des choses qu'on ne sait pas faire et qu'on a besoin d'essayer de faire sur des grands nombres. Par exemple, il y a un problème depuis x temps, c'est la répartition des nombres premiers, ça on a quelques résultats mais peu. Et donc, il y a des gens ici qui ont fait tourner des programmes, pendant un an ils regardaient les résultats 2-3 fois par semaine pour voir ce que ça donnait mais… Alors maintenant quels sont les problèmes que ça pose, il y en a plein, mais posez-moi des questions !

En fait, au départ on est parti de ce 4CT, mais pour en sortir. En fait, on s'intéressait à la controverse initiale sur l'acceptation des premières preuves du 4CT, et maintenant on s'intéresse plutôt à la mutation de ces démonstrations et dans quelles mesures ces démonstrations, qui peuvent être monstrueuses grandes et parfois par disjonction de cas, à quel point elles sont acceptées par les mathématiciens, et s'il y a des restes de controverse sur ces types de preuves, sur leur acceptation. Et après, du coup on s'est intéressé aux preuves prouvées par informatique, et on a remarqué que le débat se déportait sur les vérificateurs de preuve, et on s'est rendu compte que le débat n'était plus sur la preuve en elle-même mais sur le vérificateur de preuve, et voir dans quelles mesures le débat est toujours actuel sur l'acceptation de la preuve.

Oui, alors le débat, c'est complexe parce qu'il y a toujours un aspect, que je serai tenté d'appeler philosophique, c'est-à-dire un aspect qui est que même si c'est pas effectué par un esprit humain, il faut qu'on puisse se dire qu'un esprit humain à une puissance décuplée pourrait effectuer ces preuves, c'est-à-dire que les mécanismes mis en jeu par la machine sont de mécanismes qui affectent n'importe quelle intelligence, qui portent n'importe quelle intelligence, même l'intelligence humaine, de telle sorte qu'il n'y a aucun mystère qui se passe dans la machine, ou que si mystère il y a, il pourrait être éclairci. C'est un problème réel, car ce n'est pas clair que ce mystère puisse être éclairci, ce n'est pas clair que parce qu'il y a machine, un esprit humain arriverait à refaire toutes les différentes trajectoires qui sont

proposées par la machine. Ça c'est une chose difficile, et d'autre part il y a une controverse qui est plus profonde, pour moi, épistémologiquement, c'est-à-dire est-ce que la machine raisonne et produit des raisonnements aussi subtils que pourrait le faire un mathématicien, et ça c'est pas du tout clair. Si vous voulez, l'idée c'est de dire est-ce que les preuves par machine ne sont pas des preuves par corrélation ou par coïncidence. Il y a démultiplication d'une combinatoire, quelle que soit sa subtilité, et si on dit que ça ce sont des maths, on dit que d'une certain manière les mathématiques sont une gigantesque combinatoire, or on peut discuter longuement là-dessus, voir même on peut dire que les mathématiques sont une gigantesque algorithmique, et ce n'est pas vrai non plus. Cela étant, il se pose quand même un problème, j'ai des collègues qui pensent que si les mathématiques ne sont pas une gigantesque algorithmique, il n'empêche qu'il n'en reste pas moins qu'une preuve ou une démonstration transparente doit pouvoir se réduire à une algorithmique. Vous avez un théorème qui est assez fameux en géométrie différentielle, qu'on appelle le théorème extraordinaire, qui est un théorème de Gauss qui démontre que la courbure d'une surface prise dans est intrinsèque, c'est une notion métrique, comme serait une intégration... Pour démontrer ce théorème, Gauss est passé par un calcul extraordinaire, extrêmement compliqué pour l'époque, pour le XIXème siècle, Gauss était un calculateur prodige, et quand on suit de très près la démonstration, on voit qu'il y a une certaine inventivité. Cela étant, quand vous regardez dans les manuels de niveau recherche, la transcription de cette preuve, elle se termine presque toujours par un algorithme, les gens disent voilà maintenant on peut vous donner un algorithme qui va vous calculer la courbure, c'est-à-dire que le rapport à l'algorithme est complexe. Et puis, il y a des algorithmes subtils aussi, mais ça dépend à quel niveau on est, si on est sur le hardcore ou pas !

C'est intéressant ce que vous dites, parce que pendant un moment, en s'intéressant à ce problème et à ces débats, on s'est posé la question de savoir si les débats autour de la notion de preuve, ce n'était pas justement un débat qui se centrait autour des philosophes, voir des sociologues, et dans une certaine mesure, les mathématiciens trouvaient ça secondaire. Est-ce que vous pensez que cette affirmation est vraie ou qu'il y a quand même une présence des mathématiciens dans le débat ?

Oui, il y a une présence des mathématiciens à tous niveaux, quand même. D'abord si on prend le cas de ce qui maintenant redevient à la mode, qui est l'IA. Il y a quelques jours, il y avait un colloque avec le beau monde politique, Hollande, etc, et on s'est rendu compte qu'il y a une prise de participation encore plus grande des mathématiciens, encore plus que ce qu'elle était avant. Donc les mathématiciens sont là pour proposer des modèles mathématiques et donc ils ont quelque chose à dire de ce point de vue-là, même dans l'utilisation des calculs et même dans la manière d'utiliser les calculs. Et puis, il y a une discipline qu'on appelle, je crois, la morphologie mathématique ou l'imagerie mathématique, la manière qu'on a de faire la reconnaissance des formes, tout ça se développe aussi. Il y a pas mal de mathématiques dedans, il y a de la topologie, de l'analyse, de l'arithmétique, donc de ce point de vue-là, les mathématiciens sont là, et puis il y a toute la question de la cryptographie et du codage, et cette cryptographie, je dirais, elle est presque entièrement

fondée sur de la théorie des nombres. Et les codes les plus difficiles à percer sont ceux qu'on a trouvé, même des résultats qui datent de l'arithmétique de Gauss. Donc les mathématiques jouent un rôle.

Dans mon sens, c'était plus est-ce que les mathématiciens prennent part à un débat qui aurait lieu sur la nature d'une preuve mathématique ? Est-ce que les débats sur la nature d'une preuve sont plus du point de vue philosophique ou du point de vue mathématique ?

Je crois que c'est les deux, mais vous avez des preuves très célèbres, par exemple la preuve de Fermat, qui a eu lieu il y a 5-6 ans, c'est une preuve qui est entièrement du fait des mathématiciens, et on pourrait dire qu'une grande partie du corpus mathématique contemporain participe à cette preuve. Il y a toutes les disciplines, de l'analyse, de l'arithmétique, de la géométrie, de la géométrie algébrique, etc… Donc la combinaison de toutes ces disciplines, qui produit la preuve, c'est l'objet des mathématiciens et même la contestation de la preuve, elle vient des mathématiciens, la philosophie, je dirais, pose des questions différentes. Comment on pourrait qualifier ces questions ? **Pour les mathématiciens, c'est la question de la forme d'adhésion, de conviction que la preuve l'emporte, et c'est toute la communauté qui se met d'accord,** jamais ou très rarement dans l'histoire il y a eu qu'une partie de la communauté accepte et l'autre partie refuse. Il y a des choses comme le théorème P = nP, qui reste une conjecture, il y a des gens qui prétendent l'avoir démontré, d'autres qui prétendent que non, et quand on a fait vérifier dans des revues, ils n'ont jamais pu trancher parce qu'ils étaient à égalité. Mais là c'est plutôt du côté des mathématiciens. Du côté des philosophes c'est plus complexe, parce que du côté des philosophes, il y a d'abord la question de l'accession aux objets, les objets mathématiques sont tellement compliqués que pour qu'un philosophe y ait accès, ce n'est pas sa culture, donc il faut vraiment qu'il arrive à travailler. Et puis après se pose la question de savoir comment l'intuition joue-t-elle un rôle, comment la déduction s'effectue, quelle sorte de déduction, etc… Mais je ne pense pas, peut-être que je me trompe, que la question de la remise en cause de la preuve soit un problème. Il y a des problèmes, par exemple il y a des preuves de nature différente, par exemple la démonstration par l'absurde. On va dire est-ce qu'une démonstration par l'absurde c'est mieux qu'une démonstration directe ? Ça dépend, et là, il y a des positions philosophiques différentes. Vous avez les gens qui sont constructivistes, il y a aussi des mathématiciens qui sont constructivistes, ils veulent que l'objet soit construit directement, qu'on y ait accès mentalement, qu'on puisse le voir dans sa construction, et pour eux c'est mieux d'avoir une preuve directe. Maintenant, il y a une autre forme de conviction, c'est que les démonstrations par l'absurde ça suppose qu'on accepte, et ça tout le monde l'accepte, qu'il y ait un principe de non-contradiction. A partir du moment où vous demandez que ce soit non-contradictoire, vous être presque obligé d'accepter les déductions du type déduction par l'absurde.

Pourtant il y a certains mathématiciens qui refusent, j'ai vu certaines positions qui évitaient les preuves par l'absurde, justement parce qu'il y a une branche des mathématiques qui refuse cette forme de déduction.

Oui, au nom du caractère constructif des mathématiques. **Après il y a d'autres questions qui se posent, ce sont, pour moi, des questions très importantes, qui est la diffusion d'une preuve dans la communauté en générale. Ça suppose qu'une fois qu'une preuve a été trouvée, il y a un re-travail qui se fait sur la preuve qui peut durer assez longtemps, pour la simplifier un maximum pour qu'elle puisse être comprise et transmise par et auprès de non-spécialistes.** Ça peut être des preuves, ça peut être de grandes entreprises de classification, parce que les mathématiques c'est beaucoup une entreprise de classification des objets. Quand vous avez la classification des groupes finis, ça a été fait par des mathématiciens et c'est une classification qui a due être comprise par une dizaine de personnes au monde. Alors ça pose problème quand même, après on va utiliser ces résultats mais on fait confiance, donc…

Mais du coup dans le cas où la preuve est informatique ? Il y a aussi un problème d'accessibilité et de relecture de cette preuve, qui ne peut être faite que par un ordinateur en étant réexécutée…

Oui et bien, c'est ce qu'on appelle des preuves de réécriture. Mais il y a toutes sortes de méthodes, il y a ce qu'on appelle les preuves par transparence… Alors effectivement ça suppose une sorte de méta programme, vous réécrivez un programme qui est la réécriture de la preuve mais pas dans tous ses détails, dans ses aspects essentiels. Et ça, c'est un travail compliqué. A ma connaissance, ce n'est pas le cas pour la preuve de Fermat, et elle est encore diffusée, cette preuve fait l'objet de cours pour les gens de 3e cycle, même plus, mais elle n'est pas encore suffisamment diffusée, suffisamment comprise pour que ça fasse l'objet d'un cours de licence. Mais l'idéal c'est ça. A mon époque, la théorie de Galois c'était un cours de maîtrise, de 4e année, maintenant ça se fait même en 1ère année, alors ça dépend du niveau des gens bien-sûr. **Il y a aussi cet aspect que la preuve, plus elle est simple, plus elle est simplifiée, et plus elle est transmissible. C'est un travail sociologique à l'intérieur des mathématiques que de travailler à la simplification des preuves**. Ça remonte à loin parce que vous avez des tempéraments de mathématiciens très différents. Par exemple, quand Grothendieck écrivait les éléments de géométrie algébrique, il les écrivait comme ça, et derrière il y avait Dieudonné qui repassait et qui rédigeait. **Donc vous avez des mathématiciens qui rédigent et des mathématiciens qui inventent, et ce n'est pas forcément les mêmes.**

Au tout début de nos recherches, on pensait qu'il existerait encore une controverse sur l'acceptation des preuves informatiques puis, en reprenant l'histoire des mathématiques, de la logique, et en s'intéressant aux théorèmes d'incomplétude de Gödel, on a vu que le débat n'avait plus lieu d'être parce qu'on savait qu'il y avait

certains théorèmes qui pourraient ne pas être prouvés, c'est-à-dire qu'on ne pouvait pas forcément démontrer certains théorèmes dans un système d'axiomes définis.

Oui c'est vrai, mais ce n'est pas le cas de Gödel. Gödel démontre qu'on ne peut pas démontrer que l'arithmétique est non-contradictoire, l'arithmétique élémentaire, mais c'est un théorème. Au début il l'a démontré de façon très dure, maintenant on a simplifié la démonstration, mais les gens qui lisaient ça en 1930-1935, ils n'arrivaient pas à lire, parce qu'il y a un nombre de définitions préalables. Et puis après ça a été simplifié. Puis après, il y a la version informatique, la version de Turing, ce qu'on appelle le problème de l'arrêt, et ça c'est accessible, donc il n'y a pas de controverse là-dessus.

Oui, c'est surtout sur notre sujet d'études : après on a rencontré des informaticiens, notamment ceux qui ont travaillé sur le théorème de Feit-Thompson, le 4CT qui ont justement été prouvés par des assistants de preuve. Ils nous ont réorienté vers d'autres travaux, qui tiennent à la théorie des types, et on a a vu qu'il y avait un livre qui était sorti dans les années 2012-2013, et on se demandait si ce n'était pas l'émergence d'une théorie qui allait compléter tout ce qui est théorie des ensembles, un système plus puissant qui permettrait de démontrer plus de choses en restant crédible.

Oui, bien sûr mais en un sens, il y a plus puissant que la théorie des ensembles, qui est la théorie des catégories, qui d'une certaine manière englobe la théorie des ensembles. Justement à l'intérieur de la théorie des catégories, vous avez la théorie des types, qui a d'abord été une version de la théorie des ensembles pour éviter les paradoxes, et puis maintenant elle est intégrée à la théorie des catégories. Dans le cadre de la théorie des catégories, on peut fabriquer, il y a des algorithmes … On sait qu'un calcul élémentaire, c'est une catégorie, donc on peut traduire à l'intérieur de cette catégorie, donc ça aide beaucoup, ça c'est vrai.

C'est pour ça qu'on se demandait si ce problème de démontrer des choses dans des systèmes d'axiomes, dont on ne peut pas prouver s'ils sont contradictoires ou non, ça n'avait pas évolué. On a vu des travaux récents de Voevodsky qui a eu la médaille Fields en 2002, et qui présentait ses travaux en montrant que le calcul comme c'est un objet de la théorie, il pouvait nous affirmer qu'une preuve était valable même si on ne pouvait pas démontrer que le système d'axiomes était non-contradictoire.

C'est compliqué, ça dépend comment on interprète parce qu'il a réussi en quelque sorte à rendre le calcul relativement indépendant par rapport à l'axiomatique, donc il y a des gens qui ont dit que cela voulait dire que l'axiomatique de Peano, qui est l'axiomatique de l'arithmétique, est contradictoire. Non ça ne veut pas dire ça, ça veut dire que d'une certaine manière on peut s'en passer, mais dans le cadre d'une théorie hyper puissante qui est la théorie homotopique. Mais la théorie de l'homotopie c'est compliqué, ça relève de la topologie algébrique, des questions de déformation, donc c'est ça qui s'est passé, c'est-à-dire que le calcul est en quelque sorte absorbé par un modèle qui est plus puissant que lui mais qui en

même temps le dynamise. Par exemple, si vous prenez la conjecture de Syracuse, on peut dire qu'on n'est pas encore capable de la faire parce qu'on n'a pas les maths qui faut mais avec les catégories, on peut s'en rapprocher. Et c'est très joli parce qu'en général ces problèmes de calcul sont posés de façon extrêmement simple et en fait on s'aperçoit que dessous il y a des choses très compliquées. Mais ce que vous dites est vrai, c'est-à-dire que le développement de la théorie des catégories et d'une certaine partie de la théorie des catégories qu'on appelle la théorie des topos, ça permet d'avoir prise sur des calculs, de se faire une idée conceptuelle des calculs.

En revenant sur la preuve, on parlait du fait que ce qui était important c'était de la simplifier pour que tout le monde puisse la comprendre, est-ce que du coup ça pose la question du langage ? Est-ce qu'en ce sens le langage devient important en maths, pour comprendre les preuves ?

Oui tout à fait, bien sûr. D'abord, il faut qu'on s'entende sur les concepts. Malheureusement, et les gens ne le savent pas, mais souvent les mathématiciens n'appellent pas du même mot la même chose, et ça c'est élémentaire. Maintenant, le langage qu'on invente, qu'on construit, on le construit au fur et à mesure qu'on construit la théorie, et ça c'est difficile à trouver, et c'est une véritable création, c'est presque comme la création poétique, si vous voulez. Si un jour vous étudiez l'œuvre de Grothendieck, il est particulièrement talentueux pour trouver des mots, des concepts qui sont extrêmement évocateurs. Mais, là je parle du caractère imagé du langage mathématique, si vous regardez la théorie des anneaux, les anneaux c'est une structure algébrique assez compliquée parce qu'il y en a peut-être une trentaine de sortes différentes, les anneaux noethériens, factoriels, principaux, etc, et il y a des anneaux qu'on appelle assassins, parce qu'ils ont une manière de détruire, quand on les pose sur des objets, ils les avalent. Vous avez en théorie des faisceaux, c'est une théorie en géométrie algébrique qui s'est développée au début du XXème siècle, qui est une théorie hyper-puissante, en gros on pose la différence entre ce qui est local et ce qui est global, donc en mathématiques on va définir ce que c'est la localité; et bien les faisceaux il y en a plein, de toutes sortes, il y a les faisceaux mous, les faisceaux fi-mous, les faisceaux gratte-ciels, les faisceaux pervers, donc vous voyiez, **il y a toute une faune d'objets et c'est sans doute le langage mathématique qui comporte le plus d'objets, et de mots différents**. Si vous comparez avec une autre discipline, même la biologie n'a pas autant de mots que les mathématiques. De ce point de vue, il faut effectivement un langage commun, et apprendre. Quand vous commencez à apprendre une théorie mathématique, vous commencez par apprendre toutes les définitions et vous voyez, il y a des mots qui sont très très différents, et qui le plus souvent sont très évocateurs. Donc ça c'est la question élémentaire du langage, après il y a le langage en tant que transmetteur, en tant que véhicule de l'information, mais en général de ce point de vue là, il est corrélé à la définition et donc il y a des définitions qui vont ensemble. Par exemple, vous avez un mathématicien, celui qui en gros a inventé la géométrie projective au XVIIème siècle, qui est Desargues; tout ce que vous appelez les coniques, les hyperboles, paraboles, cercles, etc, il a voulu leur donner un nom, qui était un nom tiré de la botanique, donc il appelait ça des troncs, des feuilles et il a essayé de diffuser ce langage, mais ça n'a pas pris dans la communauté pour toutes sortes de raisons. Donc le langage est

compliqué et pour le langage mathématique, il faut à la fois jouer sur son caractère métaphorique évocateur et sur sa rectitude, son exactitude. Et c'est à ces deux exigences qu'il faut pouvoir répondre.

Sur la question d'élégance d'une preuve, beaucoup disaient que la preuve du 4CT n'était pas acceptée parce qu'elle est trop brute et pas assez élégante étant donné que c'est une énorme disjonction de cas, où on traite chaque cas. Est-ce qu'il y a une acceptation générale des critères d'élégance ?

Bien sûr, mais cela dit ce n'est pas un critère d'élimination. Il y a une dimension esthétique absolument nécessaire, non seulement dans la preuve, mais dans les mathématiques ; vous avez des mathématiciens qui écrivent des mathématiques de manière élégante, etc. Et effectivement, l'élégance d'une preuve, après il faudrait discuter philosophie, **est-ce que c'est un critère esthétique qui est lié par exemple à la simplicité ? Pas forcément, il peut y avoir du compliqué qui est élégant. Il y a aussi l'élégance par rapport à la trajectoire d'une preuve : dans le cas d'une disjonction de cas, il y a des effets de monotonie,** qui font que l'esprit a tendance à s'endormir, et ça devient pédestre, on fait des choses qui non plus aucune inventivité. **Donc l'élégance, elle est aussi la marque d'un style, et d'une inventivité de la part du mathématicien qui a trouvé la preuve.** Cela tient à un autre phénomène important, qui est que **dans de très nombreux théorèmes importants vous avez plusieurs démonstrations :** le théorème fondamental de l'algèbre, qui est un gros théorème, Gauss est a donné 4 preuves, dont une qui est faite à 50 d'écarts, et chacune d'elle a son importance. Par exemple, le théorème de l'infinité des nombres premiers, il en existe une quinzaine de preuves et on peut comparer chacune d'elles. **Outre le critère d'élégance, il y a la quantité de mathématiques intéressantes que véhicule chaque preuve. Une preuve c'est aussi une force de pénétration dans l'ensemble du corpus mathématique, et plus vous arrivez à trainer, à accrocher des objets, des champs, des domaines, meilleure votre preuve est, à condition évidemment qu'elle n'exige pas des connaissances que seulement une petite minorité des mathématiciens pourraient avoir.** Ce qui fait bouger et vivre les mathématiques c'est que tout est utile, tout a son rôle.

On se posait la question de savoir pourquoi il y a toujours des gens qui essaient de prouver avec un papier, un crayon le 4CT encore aujourd'hui lors qu'il y a une acceptation de la preuve informatique.

C'est plus un phénomène psychologique et qui relève de la philosophie, c'est-à-dire que d'une certaine manière **la machine est vue comme quelque chose d'étranger à l'homme, qui est dépossédé par cette machine, et par conséquent il refuse d'être dépossédé, même si cet objet lui apporte beaucoup.** C'est comme les gens face au pilote automatique, vous avez des ordinateurs qui conduisent l'avion et à un moment donné le pilote veut reprendre la main parce que c'est l'intelligence humain qui devrait faire le travail et c'est comme ça qu'il se crash. **Donc c'est plutôt ce refus qui vient du sentiment d'être dépossédé de ses propres facultés intellectuelles par un objet étranger.**