

Les mystères de MU, le théorème oublié

Valvassori Moïse

Sun Nov 10 17:57:36 2002

L'ordinateur calcule ce qu'on lui demande de calculer : une belle évidence. Et pourtant : tout est-il calculable ? Supposons que l'on vous demande de calculer la valeur du mille milliardième nombre premier. Vous répondrez vraisemblablement, et à juste titre, que vous savez le faire, mais que, pour réussir, vous exigerez quelque menue monnaie : de quoi acheter, installer, et faire fonctionner pendant quelques mois une belle machine, comme un Cray.

Maintenant, le même «on» vous propose, de son sourire diabolique, de démontrer par le calcul le dernier théorème de Fermat. Il est simple : «*Pour tout $n < 2$, l'identité $x^n + y^n = z^n$, ou x, y , et z sont entiers, n'a pas de solution*».

Intuitivement, et pas seulement parce que trois siècles n'ont pas résolu la question, vous sentez que l'ordinateur ne vous est d'aucun secours. Le problème de Fermat est-il calculable ou non ? Nul n'en sait rien.

Et voici le problème de MU. Considérons un système qui ne comprend que trois symboles M, I, et U. MI, MU, MM, UM, IM, IMM, sont des «*chaînes*» valides dans le système. Un «*théorème*» est une chaîne que l'on peut déduire d'un «*axiome*», c'est-à-dire d'une chaîne donnée à priori, au moyen de «*règles*». Une «*règle*» permet de passer d'une chaîne à une autre.

Travaux pratiques

- Un axiome : MI
- Quatre règles :

1. si une chaîne se termine par I, on peut lui ajouter un U en fin : MI donne MIU ;
2. d'une chaîne de type Mx (où x est une sous-chaîne), on peut faire une chaîne Mxx : MI donne MII ;
3. si, dans une chaîne, on trouve trois I de suite : III, on a le droit de les remplacer par un U : MIII donne MU
4. si, dans une chaîne, on trouve deux U, on a le droit de les abandonner : UUU donne U.

De ces règles, assez proches, si l'on y réfléchit, de celles de la géométrie euclidienne, ou de l'arithmétique classique, on tire facilement quelques intéressants théorèmes, démontrables de plusieurs manières, comme tout bon théorème.

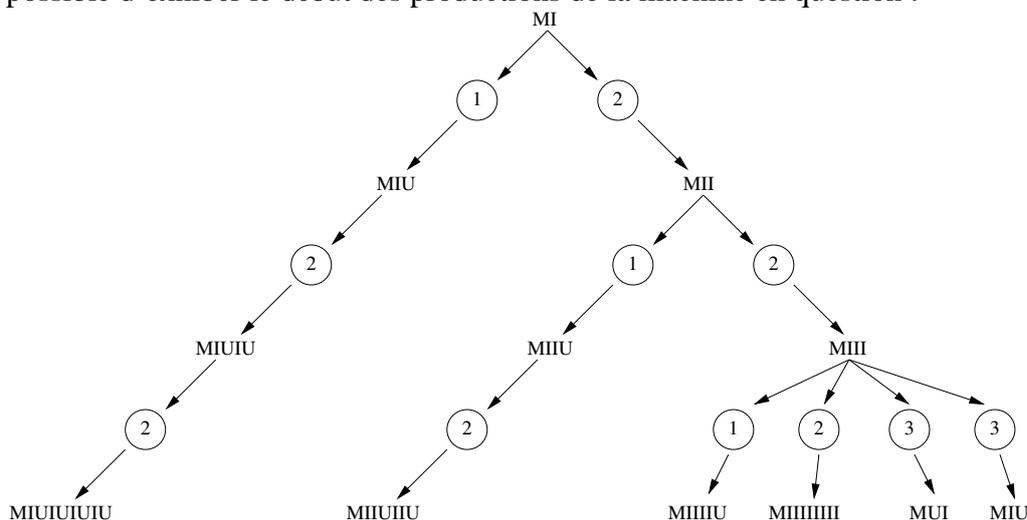
Exemple : *MIU est un théorème.*

1. de MI (axiome), on tire MIU par la règle 1
2. de MI (axiome), on tire MII par la règle 2 puis MIII toujours par la règle 2 et enfin MIU par la règle 3.

Le problème est alors simple : «MU » est-il un théorème du système ?

N'oublions pas que MU est une chaîne valide, étant composée de deux symboles du système. Les petits malins conclueront même que MU est d'autant plus valide que, partant de l'axiome MI, les règles 1, 2, 3 et 4 ne permettent que des théorèmes commençant par M. Mais cela ne suffit pas, tout malins qu'ils soient, à démontrer MU.

Que le lecteur réfléchisse : il est possible de programmer une machine pour produire *tous* les théorèmes, à condition qu'elle travaille aussi longtemps que l'on veut. Ce n'est pas très difficile, il est possible d'exhiber le début des productions de la machine en question :



Quand produira-t-elle le théorème MU ? La réponse est «jamais», et elle est facile à prouver, à condition d'utiliser un autre système de production de théorèmes, bien connu sous le nom d'«arithmétique».

La chaîne MU comprend zéro I. Zéro est un multiple de 3 (rappelons au passage que $3 \times 0 = 0$). Considérons le nombre de I autorisé : les règles 1 et 4 les laissent inchangé. La règle 3 diminue le nombre de I de 3, elle ne le change donc pas quant à la divisibilité par 3. La règle 2 double le nombre de I ; comme $2n$ ne peut être divisé par 3 que si n est divisible par 3, la règle 2 ne produit pas de multiple de 3. Donc aucune règle ne produit de multiple de 3.

L'axiome MI contient un nombre non multiple de 3 de I : 1. Donc aucun théorème ne peut contenir de multiple de 3 de I, donc en particulier zéro I. MU n'est donc pas «démontrable» dans le système MIU. Simple, n'est-ce pas ? Mais nous avons du avoir recours à ce que les mathématiciens appellent un «méta-système» : l'arithmétique classique, qui elle-même possède ses propres axiomes et règles... avec lesquels il n'est pas possible de démontrer certains théorèmes sans recours à un nouveau «méta-système» (si MU n'est pas démontrable dans le système MIU, la fausseté de MU n'est pas non plus démontrable, il faudrait pour cela balayer tout l'arbre issu de MI... Or MU, nous l'avons prouvé par l'arithmétique, est faux).

Seule conclusion possible de ce jeu de miroirs à l'infini : tout ce qui est vrai n'est pas obligatoirement calculable, et de ce qui n'est pas calculable, il est impossible de dire si c'est vrai ou non.

Mathématiciens, informaticiens, soyons humbles.

Si vous voulez en savoir plus sur le théorème MIU, je vous conseille de lire l'excellent livre de Douglas Hofstadter, "Gödel, Escher, Bach - Les brins d'une guirlande éternelle" paru en France chez InterEditions.