5. ATTENTION AUX GÉNÉRALISATIONS HÂTIVES

De nombreuses fois dans l'histoire des mathématiques, des propriétés constatées sur un petit nombre de cas ont été conjecturées «vraies dans tous les cas». Voici quelques exemples de situations qui montrent qu'il faut se méfier de telles généralisations.

(a) Pierre de Fermat considère l'expression $F_n = 2^{2^n}+1$ et, après le calcul de F_0, F_1, F_2, F_3, F_4, constate qu'il s'agit toujours de nombres premiers. Il en tire la conjecture que F_n est toujours un nombre premier. Le grand Leonhard Euler découvre plus tard que F_5 n'est pas premier. Pire : aujourd'hui, après avoir évalué et testé les valeurs suivantes de F_n, on n'a trouvé que des nombres composés. On se demande donc si, au-delà de F_5, tous les F_n ne seraient pas composés ! Si c'est le cas, ce sera l'exemple extrême de la conjecture fausse : non seulement elle possède un contre-exemple, mais tout nombre plus grand que 5 est un contre-exemple !

(b) Plus récemment, on a remarqué que :

3! – 2! + 1! = 5 : premier
4! – 3! + 2! – 1! = 19 : premier
5! – 4! + 3! – 2! + 1! = 101 : premier
6! – 5! + 4! – 3! + 2! – 1! = 619 : premier
7! – 6! + 5! – 4! + 3! – 2! + 1! = 4 421 : premier
8! – 7! + 6! – 5! + 4! – 3! + 2! – 1! = 35 899 : premier

En conclut-on que $n!$ – $(n–1)!$ + ... + $(–1)^n$ 2! – $(–1)^n$ 1! est toujours un nombre premier ?

Non : 9! – 8! + 7! – 6! + 5! – 4! + 3! – 2! + 1! = 326 981 = 79 × 4 139.

(c) Plus étonnant encore est l'exemple suivant. Les nombres n^{17} + 9 et $(n + 1)^{17}$ + 9 n'ont pas de facteurs communs si n = 1, n = 2, n = 3, etc. Vous pouvez vérifier cela jusqu'à 100, jusqu'à 1 000, jusqu'à un milliard, jusqu'à mille milliards de milliards, et même jusqu'à huit millions de milliards de milliards de milliards de milliards de milliards. Pourtant, un peu plus loin, pour :

n = 8 424 432 925 592 889 329 288 197 322 308 900 672 459 420 460 792 433 ≃ 8,424 10^{52}, vous rencontrerez une exception : parfois n^{17} + 9 et $(n+1)^{17}$ + 9 ont des facteurs communs.

(d) Il est des situations plus étranges encore, où seul le raisonnement permet de savoir qu'une propriété toujours testée vraie en pratique est fausse en général.

L'exemple le plus connu est celui qui concerne l'approximation de Pi(m) le nombre de nombres premiers inférieurs à m. On sait que ce nombre vaut à peu près :

$$\mathrm{Li}(m) = \int_2^m 1/\log(x)\,dx\ .$$

On constate en pratique que Pi(m) ≤ Li(m), et l'on ne connaît aucune exception à cette inégalité. Cependant le mathématicien Littlewood a prouvé en 1914 que la quantité Pi(m) – Li(m) changeait de signe une infinité de fois, et donc qu'il n'est pas vrai que Pi(m) ≤ Li(m) pour tout m. En 1933, S. Skewes a établi que le premier changement de signe se produit avant $10^{10^{10^{34}}}$ (quatre niveaux d'exposant). Cette majoration a été améliorée par H. te Riele, en 1987, par 10^{371}, mais c'est encore au-delà de ce qu'on peut atteindre numériquement : aujourd'hui, on sait qu'il existe un m tel que Pi(m) > Li(m), mais on n'en connaît aucun.

```
      if d*d>p then k:=k+1;fi;
    od;
    p;
  fi;
end:
```

Ce qui tient sur cinq lignes :

```
premier := proc(n) local p,k,d;if n=1 then 2 else p:=1;k:=1;while k<>n do p:=p+2;d:=2;while(d*d<=p)and(p mod d <> 0)do d:=d+1;od;if d*d>p then k:=k+1;fi;od;p;fi;end;
```

Explications : proc est un mot convenu pour indiquer qu'on définit une procédure, c'est-à-dire une fonction ; local sert à préciser les variables qu'on utilisera dans le calcul ; if C then A1 else A2 fi est la structure de contrôle qui, lorsque la condition C est satisfaite, exécute l'action A1 et qui, sinon, exécute l'action A2 ; while C do A od est la structure de contrôle qui, tant que la condition C est satisfaite, exécute de manière répétée l'action A ; end indique la fin de la définition de la procédure.

Le programme, si n vaut 1, donne 2. Sinon, en parcourant les entiers de 2 en 2 (variable p), le programme recherche les nombres premiers et les compte avec la variable k, jusqu'à en avoir trouvé n. Le programme rend alors le résultat p, qui à cet instant, contient bien le n-ième nombre premier.

On peut faire encore plus court, mais cette définition possède plusieurs avantages sur la définition mathématique précédente de p_n ou sur une définition plus courte en Maple : elle se comprend immédiatement pour qui possède quelques connaissances du langage Maple, elle est fondée sur l'idée la plus naturelle qu'on puisse avoir ; elle permet de calculer en quelques secondes le centième nombre premier, et même le millième.

La recherche de formules n'utilisant qu'un symbolisme mathématique limité est un jeu un peu gratuit que les mathématiciens professionnels regardent le plus souvent avec amusement sans le prendre au sérieux (ce qui n'empêche pas que d'éminents mathématiciens comme G. Hardy ou E. Wright s'y soient adonnés).

6. FORMULES SIMPLES DONNANT DE GRANDES QUANTITÉS DE NOMBRES PREMIERS

Certaines formules, sans donner tous les nombres premiers, ni même ne donner que des nombres premiers, en donnent une grande quantité en suivant. C'est le cas de la formule d'Euler $f(n) = n^2 – n + 41$, qui donne des nombres premiers pour toutes les valeurs de n allant de 0 à 40.

Les polynômes suivants battent le record d'Euler :

$103n^2 – 3945n + 34381$ est premier pour n = 0, 1, ..., 42 (R. Ruby).

$47n^2 – 1701n + 10181$ est premier pour n = 0, 1, ..., 42 (G. Fung).

$36n^2 – 810n + 2753$ est premier pour n = 0, 1, ...,44 (R. Ruby).

Une conjecture très vraisemblable (car liée à une autre bien testée) est qu'aussi grand que soit A on peut trouver un polynôme de la forme $n^2 + n + B$ qui donne des nombres premiers pour n = 0, ..., A. On sait cependant que B sera nécessairement très grand : la valeur de B correspondant à A = 41 est plus grande que 10^{18}, mais reste inconnue.