Théorème

La fonction f définie sur N^2 à valeurs dans R par :

$$f(x,y)=\frac{y-1}{2}\left[\left|[x(y+1)-(y!+1)]^2-1\right|-\left([x(y+1)-(y!+1)]^2-1\right)\right]+2$$

engendre uniquement des nombres premiers, tous les nombres premiers, et chaque nombre premier impair exactement une fois.

remarque : f n'est pas une bijection de N^2 sur l'ensemble P des nombres premiers car elle donne 2 très souvent. En revanche, et c'est remarquable, c'est une bijection de N^2-{$f^{-1}(2)$} sur P-{2}.

démonstration

Posons B=x(y+1)-(y!+1).

1. B est entier et donc B^2 également. On a donc soit $B^2=0$, soit $B^2\geq 1$.
   Si $B^2\geq 1$, f(x,y)=2 qui est bien premier.
   Si $B^2=0$, f(x,y)=y+1, qui est entier.
   Donc f ne donne que des entiers.
2. D'après 1., on pourra supposer dans toute la suite que $B^2=0$ et donc que B=0.
   On a donc x(y+1)=y!+1 et ainsi y+1 divise y!+1. D'après le **théorème de Wilson**, y+1 est donc premier.
   Donc f ne donne que des nombres premiers.
3. Soit p un nombre premier distinct de 2. On cherche un couple (x,y) d'entiers naturels tel que f(x,y)=p.
   Comme B=0, cela revient à y+1=p et donc à y=p-1, qui est entier. D'autre part, comme B=0, x(y+1)=y!+1.
   Ainsi, xp=(p-1)!+1 et, par suite, $x=\frac{1}{p}\left[(p-1)!+1\right]$, qui est entier d'après le **théorème de Wilson**. Le couple $\left(\frac{(p-1)!+1}{p};p-1\right)$ est donc un antécédent de p par f.
   Donc f donne tous les nombres premiers.
4. Il reste à montrer que le couple précédent est unique (il faut prendre garde au fait que f ne donne pas 2 *uniquement* si $B^2\geq 1$, car, par exemple, f(1,1)=2). Si B=0, f(x,y)=y+1 ou f(x,y)=2. Dans ce dernier cas, y=1 et donc x=1. (1,1) est donc le seul couple à avoir pour image 2 lorsque B=0. Si p n'est pas égal à 2, f(x,y)=p si et seulement si y+1=p. Ainsi, y=p-1 est fixé. Puisque B=0, $x=\frac{y!+1}{y+1}$, est également fixé. Le couple antécédent de p obtenu au 3. est donc unique.
   Donc f donne chaque nombre premier impair exactement une fois.

remarque : si l'on veut faire "fonctionner" f à l'aide d'un ordinateur, il faudra parcourir N^2 suivant le procédé diagonal, c'est à dire énoncer les couples (x,y) comme suit : (0,0) (1,0) (0,1) (0,2) (1,1) (2,0) (3,0) (2,1) (1,2) (0,3) (0,4)... et s'armer de patience !

Théorème de Wilson

p divise (p-1)!+1 si et seulement si p est premier

(théorème d'arithmétique qui sera démontré dans le supérieur à l'occasion de la théorie des anneaux puisque -snif- on ne fait plus d'arithmétique en Terminale...)