

Nelson Sp. Maths: Démonstration

T3

12/04/20

Comme Megan l'avait désiré, ce programme permet de déterminer si le nombre n est premier (sauf pour 0 et 1, exceptions que nous étudierons après cette démonstration), voyons pourquoi.

Il sera nécessaire de réaliser une séparation de cas : dans un premier temps, nous étudierons les cas où $n \geq 4$, puis les autres ensuite.

Le programme commence ainsi : il vérifie si $a \equiv p \times n \iff \forall n$.

Dans la première boucle, cette inégalité est obligatoirement vraie, puisque $p=0$, et que $\forall n \geq \sqrt{a} \geq a$ (qui vaut 1, à cet instant).

Le programme calcule alors le produit des diviseurs de n par $a^{(i/2)}$ et de n par i ($i, 3$).

Si ce produit est nul, alors l'un des deux facteurs est nul, ce qui signifie

nécessairement que n est divisible
par a ou b et donc qu'il n'est
pas premier. Dans ce cas, le
programme incrémente la valeur de
 p qui vaut alors 1.

La deuxième boucle débute alors.
Or, puisque $p=1$, $a \leq p \times n \leq \sqrt{n}$
n'est plus vérifiée, et l'on sort
de la boucle. Et puisque $p=1$,
alors le programme affiche "Non".

Si le produit précédent n'est pas nul,
alors n'est nul de la division de n par a ,
n'est nul de la division de n par b
n'est nul, ce qui signifie que
 n n'est divisible ni par 2, ni par 3.

Dans ce cas, n n'est divisible
ni par 6, multiple de 2 et 3, ni par
 $6m+2$, multiple de 2 ($=2(3m+1)$), ni par
 $6m+3$, multiple de 3 ($=3(2m+1)$), ni par
 $6m+4$, multiple de 2 ($=2(3m+2)$). n
ne peut être divisible que par $6m+5$
(ce qui revient, modulo 6, à $6m+1$), ou par
 $6m+1$.

$x=$, avec de
nouvelles valeurs

Une seconde boucle débute alors^x.
si $a \leq \sqrt{n}$, alors $a \leq p \times n \leq \sqrt{n}$
pour a, b et k (car p vaut encore 0), et l'on continue.
(Ok, Ok, Si $a \geq \sqrt{n}$, alors $a \leq p \times n \geq \sqrt{n}$, et
et $k+1$, respectivement)

l on sort de la boucle. Dans ce cas, le programme affiche "Oui", car la valeur de p est encore de 0 : on n'a trouvé aucun diviseur autre que 1 et lui-même, il est donc effectivement premier.

Dans le cas où $a \nmid \sqrt{n}$, le programme calcule une nouvelle fois le produit de toutes les divisions de n par a et n par b . S'il est nul, cela implique les mêmes choses que dans la première boucle : n est divisible par a ou b , et n'est donc pas premier, et le programme affiche "Non".

S'il n'est pas nul, alors n n'est divisible ni par a , ni par b : on repart pour une nouvelle boucle, pour les mêmes raisons que dans la première boucle.

En arrivant à cette nouvelle boucle à valeur de k , on s'arrête ainsi, puisque a et b ont la forme $5k-1$ et $5k+1$, respectivement, $k \in \mathbb{Z}$, les deux diviseurs potentiels de n .

A cet instant, deux cas sont envisageables :

- On finit effectivement par trouver un diviseur à n , on s'arrête ainsi.

l'on sort de la boucle. Dans ce cas, le programme affiche "Oui", car la valeur de p est encore ≤ 0 . On n'a trouvé aucun diviseur autre que 1 et lui-même, il est donc effectivement premier.

Dans le cas où $a \nmid \sqrt{n}$, le programme calcule une nouvelle fois le produit de toutes les divisions de n par a et n par b . S'il est nul, cela implique les mêmes choses que dans la première boucle: n est divisible par a ou b , et n'est donc pas premier, et le programme affiche "Non".

S'il n'est pas nul, alors n n'est divisible ni par a , ni par b . On repart pour une nouvelle boucle, pour les mêmes raisons que dans la première boucle.

En arrivant à l'étape nouvelle boucle à valeur de t , on s'arrête ainsi, puisque a et b ont la forme $5k-1$ et $5k+1$, respectivement, $k \in \mathbb{Z}$, tous les diviseurs potentiels de n .

A cet instant, deux cas sont envisageables:

- On finit effectivement par trouver un diviseur à n , on sort ainsi