Sylvain ETIENNE
PLC 1
etiennesy@wanadoo.fr

NOMBRES PREMIERS ; EXISTENCE ET UNICITE DE LA DECOMPOSITION D'UN NOMBRE EN FACTEURS PREMIERS. INFINITUDE DE L'ENSEMBLE DES NOMBRES PREMIERS. EXEMPLE(S) D'ALGORITHME(S) DE RECHERCHE DE NOMBRES PREMIERS. L'EXPOSE POURRA ETRE ILLUSTRE PAR UN OU DES EXEMPLES FAISANT APPEL A L'UTILISATION D'UNE CALCULATRICE.

Niveau : Terminale S.

Pré-requis : Divisibilité dans $\mathbb{N}$ – Récurrence – PGCD et PPCM –

I INTRODUCTION.

L'arithmétique a pour objet l'étude des nombres entiers et rationnels. Une particularité des entiers est les nombres premiers, qui permettent, entre autre, d'assurer le système RSA en cryptographie. Cet exposé a pour objectif de définir de tels nombres, de montrer la décomposition des entiers et enfin de voir des algorithmes de recherche des nombres premiers. Tels sera le plan de la leçon.

II NOMBRES PREMIERS.

Convention : Dans cette leçon, les entiers considérés et utilisés sont des entiers naturels, et lorsque nous parlerons de leurs diviseurs ou de leurs multiples, il s'agit toujours de diviseurs ou de multiples positifs.

A) DEFINITION.

Définition 1 :

> Un nombre premier est un entier strictement supérieur à 1, qui n'admet pas d'autres diviseurs que lui-même et l'unité.

Remarques :

- Un nombre non premier est dit composé.
- Nous généralisons la notion de nombres premiers à $\mathbb{Z}$ en convenant qu'un entier négatif est premier si son opposé est premier dans $\mathbb{N}$.

Théorème 1 :

> Tout entier a, $a \geq 2$, admet un nombre premier comme diviseur.

Démonstration :
Soit a un entier supérieur à 2.

etiennesy@wanadoo.fr

- Si a est premier, un diviseur (et c'est le seul !) premier de a est a.
- Si a n'est pas premier, a possède au moins un diviseur strictement compris entre 1 et a et nous pouvons écrire : $\mathcal{D}(a)=\{1,a_1,a_2,...,a\}$, où $\mathcal{D}(a)$ est l'ensemble des diviseurs de a, rangés dans l'ordre croissant.
  Alors a_1 est premier. En effet, par l'absurde, supposons que a_1 n'est pas premier. Alors, a_1 admet un diviseur d strictement compris entre 1 et a_1. Mais d divise a_1, et a_1 divise a, donc d divise a. Or ce n'est pas possible car a_1 est le plus petit diviseur de a strictement compris entre 1 et a. Donc a_1 est premier. □

B) ENSEMBLE DES NOMBRES PREMIERS.

Théorème 2 :

Il existe une infinité de nombres premiers.

Démonstration :

Effectuons un raisonnement par l'absurde en supposant que l'ensemble des nombres premiers $\mathcal{P}$ est fini et possède n éléments : $\mathcal{P}=\{p_1,...,p_n\}$.

Soit k l'entier naturel tel que : $k=p_1...p_n+1$.

k étant supérieur à 2, il admet un diviseur premier par le théorème 1. Notons le q. Or, aucun des entiers de $\mathcal{P}$ n'est un diviseur de k car le reste de la division de k par l'un quelconque des nombres entiers de cette liste vaut toujours 1. Donc q est strictement supérieur à p_n et est premier. Ce qui est absurde, et ainsi $\mathcal{P}$ est infini. □

III DECOMPOSITION EN PRODUIT DE NOMBRES PREMIERS.

Théorème 3 :

Tout entier naturel n distinct de 0 et de 1 se décompose de façon unique sous la forme :

$$n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}, \qquad (1)$$

où $p_1,p_2,...,p_k$ sont des nombres premiers tels que $0<p_1<p_2<...<p_k$,

et $\alpha_1,\alpha_2,...,\alpha_k$ sont des entiers naturels non nuls.

L'écriture de n sous la forme (1) est sa décomposition en produit de facteurs premiers.

Démonstration :

- Existence de la décomposition : démonstration par récurrence sur $n\in\mathbb{N}\setminus\{0,1\}$.

– Pour $n=2$, nous avons $2=2^1$ et 2 est premier ; 2 admet donc une décomposition de la forme (1).

– Soit $n\in\mathbb{N}\setminus\{0,1\}$. Supposons la propriété vraie pour tout entier naturel k tel que $2\le k\le n$, et montrons que la propriété est vraie au rang $n+1$.

Si $n+1$ est premier, alors $n+1=(n+1)^1$ est une décomposition de la forme (1).

Si $n+1$ n'est pas premier, le théorème 1 nous assure l'existence d'au moins un diviseur premier p. Nous pouvons alors écrire :

etiennesy@wanadoo.fr

$n+1=pq$ avec q entier tel que : $2\le q\le n$.

Nous pouvons appliquer l'hypothèse de récurrence à q : q admet une décomposition en produit de facteurs premiers du type (1), et donc $n+1=pq$ également, ce qui vérifie la propriété au rang $n+1$.

– En conclusion, le premier rang étant vérifié, le principe de récurrence donne l'existence d'une telle décomposition.

- Unicité de la décomposition (admise en terminale S).

Nous avons besoin d'un résultat préliminaire :

Lemme 1 :

> Si p est premier, alors $p\mid ab\Rightarrow p\mid a$ ou $p\mid b$.

Démonstration :

Si p ne divise pas a, il est premier avec a, donc p divise b par le théorème de Gauss. □

Démonstration de l'unicité par récurrence sur $n\in\mathbb{N}\setminus\{0,1\}$:

– Si $n=2$, alors la propriété est vraie (il en est de même avec tous les nombres premiers !).

– Soit $n\in\mathbb{N}\setminus\{0,1\}$. Supposons la propriété vraie pour tout entier naturel k tel que $2\le k\le n$, et montrons que la propriété est vraie au rang $n+1$.

Supposons que $n+1$ s'écrive sous les deux formes : $n+1=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}=q_1^{\beta_1}q_2^{\beta_2}...q_j^{\beta_j}$, où $p_1,...,p_k,q_1,...,q_j$ sont des nombres premiers (non ordonnés), et $\alpha_1,...,\alpha_k,\beta_1,...,\beta_j$ sont des entiers naturels non nuls. p_k divise $q_1^{\beta_1}q_2^{\beta_2}...q_j^{\beta_j}$, donc, par le lemme 1, divise l'un des facteurs, par exemple $p_k\mid q_j$. p_k et q_j étant premiers, il vient $p_k=q_j$ et nous obtenons :

$$\frac{n+1}{p_k}=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k-1}=q_1^{\beta_1}q_2^{\beta_2}...q_j^{\beta_j-1}.$$

Pour appliquer l'hypothèse de récurrence, il faut remarquer que si $\alpha_k=1$, alors $\beta_j=1$, car sinon, q_j diviserait l'un des p_i avec $i\neq k$, ce qui est absurde. De même si $\beta_j=1$, alors $\alpha_k=1$. Enfin, par contraposée, $\alpha_k>1\Leftrightarrow\beta_j>1$. Ceci montre donc que la propriété est vraie au rang $n+1$.

– En conclusion, le rang initial étant vérifié, alors par le principe de récurrence, nous avons unicité de la décomposition en produit de facteurs premiers. □

Exemple 1 :

$$\begin{aligned}360&=2\times180,\\&=2\times2\times90=2\times2\times2\times45=2\times2\times2\times3\times15,\\&=2\times2\times2\times3\times3\times5.\end{aligned}$$

La décomposition de 360 est alors :

$$360=2^3\times3^2\times5.$$

Corollaire 1 :

> Tout entier naturel $n\ge2$ non premier admet au moins un diviseur premier p vérifiant : $p^2\le n$.

Démonstration :

Avec les notations du théorème précédent, si n n'est pas premier, alors sa décomposition comporte au moins deux facteurs, éventuellement égaux à p_1, et nous obtenons la relation $n \geq p_1^2$, d'où le résultat cherché. □

IV ALGORITHME DE RECHERCHE DE NOMBRES PREMIERS.

A) PREMIER ALGORITHME.

Idée : Pour prouver qu'un nombre $n \in \mathbb{N} \setminus \{0,1\}$ est premier, il suffit de s'assurer qu'il n'a pas de diviseur inférieur ou égal à $\sqrt{n}$ (c'est une conséquence du corollaire 1).

Nous obtenons alors l'algorithme, programmé sur une T.I. Voyage 200, ci-contre qui affiche un diviseur de n s'il existe, et sinon, affiche que n est premier.

Il est formé de deux programmes (un principal et un sous-programme), le sous-programme testant la primalité du nombre n. Ce sous-programme sera à nouveau utilisé plus bas (d'où son utilité !).

```
premier1()
Prgm
ClrIO
Prompt n
prem(n)
If w=1 Then
 Disp string(n)&" est divisible par "&s
 tring(d-1)
Else
 Disp string(n)&" est premier"
EndIf
EndPrgm
```

```
prem(n)
Prgm
2→d:0→w
While d^2≤n and w=0
 n-d*int(n/d)→r
 If r=0
 1→w
 d+1→d
EndWhile
EndPrgm
```

Expérimentons cet algorithme sur les exemples suivants : 703, 733, 853.

```
n?
703
703 est divisible par 19
n?
733
733 est premier
n?
853
853 est premier
```

Cependant, dès que les nombres commencent à être grand, ce programme a l'inconvénient de tester si, par exemple, 4 et tous les nombres pairs supérieurs divisent le nombre cherché, alors que nous avons déjà fait le test de divisibilité par 2.

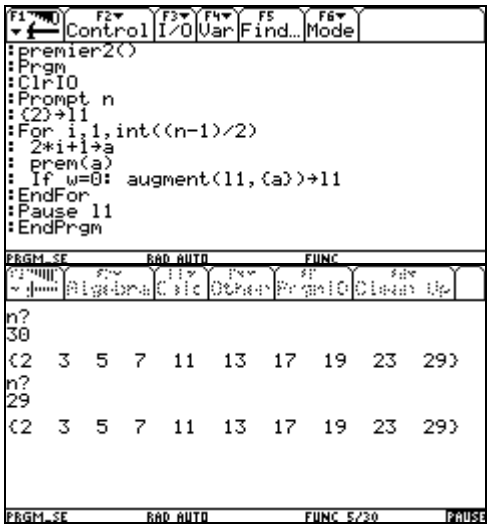
B) DEUXIEME ALGORITHME.

Idée : Pour prouver qu'un nombre $n \in \mathbb{N} \setminus \{0,1\}$ est premier, il suffit de s'assurer qu'il n'a pas de diviseur premier inférieur ou égal à $\sqrt{n}$. Il faut donc trouver tous les nombres premiers inférieurs ou égal à $\sqrt{n}$.

Ce programme utilise le sous-programme testant la primalité de i $\left(i \in \left[\!\left[1, E\left(\frac{n-1}{2}\right)\right]\!\right]\right)$, et utilise, en outre, le fait que 2 est le seul entier premier pair. Le résultat est donné sous la forme d'une liste.

Prenons par exemple 30 : nous cherchons tous les nombres premiers inférieurs à 30.

Il est à noter que 29 donne la même liste.



C) LE CRIBLE D'ERATOSTHENE.

Pour trouver tous les nombres premiers compris entre 2 et n, n étant un entier donné supérieur à 2, il faut écrire tous les nombres de 2 à n dans un tableau. Ensuite :

-*i*- nous barrons tous les multiples de 2 sauf 2 ;

-*ii*- nous barrons tous les multiples de 3 sauf 3 ;

-*iii*- le premier nombre non barré après 3 est premier, car ce nombre n'est multiple d'aucun des nombres premiers qui le précèdent. Ce premier nombre non barré est 5, donc 5 est premier ;

-*iv*- Nous barrons tous les multiples de 5 sauf 5. Le premier nombre non barré qui vient après 5 est premier, et ainsi de suite ;

-*v*- Il suffit de s'arrêter lorsque nous avons barré tous les multiples de l'entier p premier tel que $p \leq \sqrt{n}$.

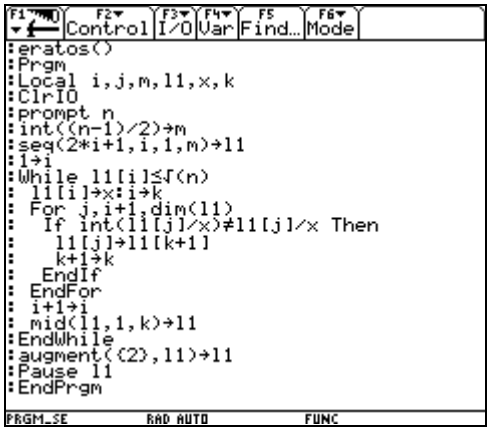
Exemple :

Avec $n = 30$, nous obtenons :

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

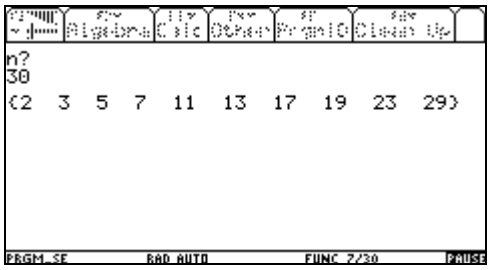
Nous nous arrêtons à $p = 5$ (car $6^2 = 36 > 30$) pour avoir tous les nombres premiers compris entre 2 et 30.

La programmation de cet algorithme est un peu plus délicate (et un peu plus longue). Nous nous intéressons aux seuls entiers impairs (2 est rajouté à la fin). Il faut prévoir une double boucle : une pour le nombre testé, et une autre pour ses multiples. Les multiples sont « écrasés » par les entiers premiers avec le nombre testé qui suivent.



Revenons à notre exemple précédent et déterminons les nombres premiers inférieurs à 30.

Nous obtenons (heureusement) la même liste que précédemment.



V UNE APPLICATION IMPORTANTE.

Le théorème 3 (dit théorème fondamental !) nous permet de déterminer le PGCD et le PPCM de deux entiers. En effet, le PGCD δ de a et b est un diviseur commun à a et b. Le théorème 3 donne la forme des diviseurs de a et de b. Nous avons alors :

$\begin{cases} a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}, \\ b = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}, \end{cases}$ où $p_1, p_2, ..., p_k$ sont des nombres premiers tels que $0 < p_1 < p_2 < ... < p_k$, et $\alpha_1, ..., \alpha_k, \beta_1, ..., \beta_k$ sont des entiers naturels éventuellement nuls.

L'entier a divise b si et seulement si $\forall i \in [\![1,k]\!], \alpha_i \leq \beta_i$. En effet, l'entier a divise b si et seulement s'il existe $c \in \mathbb{N}$ tel que $b = ac$. Notons $c = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}$ la décomposition de c. Dans ce cas, l'unicité de la décomposition en produit de facteurs premiers donne : $\forall i \in [\![1,k]\!], \beta_i = \alpha_i + \gamma_i$.

Ainsi, $d = p_1^{\gamma_1} p_2^{\gamma_2} ... p_k^{\gamma_k}$ divise à la fois a et b si et seulement si d divise $\delta = p_1^{\inf(\alpha_1,\beta_1)} p_2^{\inf(\alpha_2,\beta_2)} ... p_k^{\inf(\alpha_k,\beta_k)}$ et δ sera le PGCD de a et de b. Le même raisonnement donne le PPCM, et nous obtenons :

$\begin{cases} \text{pgcd}(a,b) = p_1^{\inf(\alpha_1,\beta_1)} p_2^{\inf(\alpha_2,\beta_2)} ... p_k^{\inf(\alpha_k,\beta_k)}, \\ \text{ppcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} ... p_k^{\max(\alpha_k,\beta_k)}. \end{cases}$

Exemple :

Trouvons grâce à cette méthode le PGCD et le PPCM de $a = 5544$ et $b = 540$.
La décomposition donne : $a = 2^3 \times 3^2 \times 7 \times 11$ et $b = 2^2 \times 3^3 \times 5$.
D'où : $\text{pgcd}(a,b) = 2^2 \times 3^2 = 36$ et $\text{ppcm}(a,b) = 2^3 \times 3^3 \times 5 \times 7 \times 11 = 83160$.

VI CONCLUSION.

Nous avons défini les nombres premiers, qui sont en nombre infini dans $\mathbb{N}$. Cela a permis de donner une décomposition en produit de nombres premiers pour tout entiers. Nous avons vu, par la suite, que savoir si un nombre est premier est un problème plutôt difficile. L'importance de tels nombres se retrouvent dans la cryptographie comme le système RSA. Il est à noter qu'émergent des algorithmes très puissants dits algorithmes probabilistes (test de Rabin-Miller, par exemple).