

LEÇON N° 13 :

Nombres premiers ; existence et unicité de la décomposition d'un nombre en facteurs premiers. Infinitude de l'ensemble des nombres premiers. Exemple(s) d'algorithme(s) de recherche de nombres premiers. L'exposé pourra être illustré par un ou des exemples faisant appel à l'utilisation d'une calculatrice.

Pré-requis :

- Définition et propriétés des ensembles \mathbb{N} et \mathbb{Z} ;
- Raisonnement par récurrence ;
- Divisibilité dans \mathbb{Z} , nombres premiers entre eux, théorème de Gauss.

13.1 Définitions et premières propriétés

13.1.1 Définition et remarques

Définition 1 : Un entier naturel n est dit *premier* s'il est distinct de 1 et n'admet pas d'autres diviseurs (dans \mathbb{N}) que les diviseurs triviaux 1 et n .

Proposition 1 : Soit $n \in \mathbb{N}^*$. Alors n est premier si et seulement si $p = ab \Leftrightarrow a = 1$ ou $b = 1$ (« ou » exclusif).

démonstration : C'est la traduction de la définition en termes mathématiques. ■

13.1.2 Trois résultats importants

Lemme 1 : Tout entier naturel supérieur à 2 possède au moins un diviseur premier.

démonstration : Soit $n \in \mathbb{N} \setminus \{1\}$. L'ensemble des diviseurs de n strictement supérieurs à 1 n'est pas vide (il contient n), donc possède un plus petit élément d . On montre que d est premier. Si a est un diviseur de d strictement supérieur à 1, alors $a \leq d$. Mais a divise n (puisque a divise d , que d divise n , et que la relation « divise » est transitive), donc $d \geq a$. Finalement, $a = d$ et les seuls diviseurs positifs de d sont 1 et d . ■

Lemme 2 : Un nombre premier est premier avec tout nombre qu'il ne divise pas.

démonstration : Si p premier ne divise pas n , l'ensemble des diviseurs de p dans \mathbb{N} sera $\{1, p\}$, et le seul diviseur commun à p et n ne peut être que 1. ■

Lemme 3 : Si p est premier, alors $(p|ab \Rightarrow p|a \text{ ou } p|b)$.

démonstration : Si p ne divise pas a , alors p est premier avec a , donc divise b d'après le théorème de Gauss. ■

13.1.3 Conséquences immédiates

Corollaire (lemme 2) :

- (i) Deux nombres premiers sont premiers entre eux ;
- (ii) Tout nombre premier p est premier avec tout $i \in \llbracket 1, p-1 \rrbracket$.

Corollaire (lemme 3) : Si un nombre premier divise un produit de facteurs premiers, alors il est égal à l'un d'eux.

13.2 Décomposition en facteurs premiers

Théorème 1 (Euclide) : L'ensemble des nombres premiers est infini.

démonstration : Supposons qu'il existe p tel que p soit le plus grand des nombres premiers. Alors $(p! + 1)$ admet au moins un diviseur premier (lemme 1) que l'on note n . Il appartient à $\llbracket 1, p \rrbracket$ (en effet, il ne peut pas être supérieur à p puisque p est le plus grand des nombres premiers). Ceci est pourtant impossible car la division euclidienne de $(p! + 1)$ par un nombre quelconque de $\llbracket 1, p \rrbracket$ est toujours de reste 1. Par conséquent, n ne divise pas $(p! + 1)$ et l'hypothèse initiale est donc fautive. ■

Remarques :

- Toute partie de \mathbb{N} étant finie ou dénombrable, l'ensemble P des nombres premiers positifs sera dénombrable. On peut l'ordonner et écrire $P = \{p_1, \dots, p_m, \dots\}$ avec $p_i < p_{i+1}$ pour tout i .

– La distribution des nombres premiers n’est pas régulière : pour tout entier naturel n non nul donné, il existe n entiers naturels consécutifs et composés. Il suffit de choisir

$$(n + 1)! + 2, \dots, (n + 1)! + n + 1,$$

et notant bien que $(n + 1)! + k$ est toujours divisible par k lorsque $2 \leq k \leq n + 1$.

Théorème 2 (théorème fondamental) : Soit n un entier naturel strictement supérieur à 1. Alors

(i) il existe k nombres premiers naturels p_1, \dots, p_k distincts deux à deux et des entiers naturels non nuls $\alpha_1, \dots, \alpha_k$ tels que $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.

(ii) il y a unicité de cette décomposition à l’ordre des facteurs près. Autrement dit,

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_m^{\beta_m}$$

entraîne $k = m$ et l’existence d’une permutation σ de $\mathbb{N}_k = \{1, \dots, k\}$ telle que $q_i = p_{\sigma(i)}$ et $\beta_i = \alpha_{\sigma(i)}$ pour tout i .

démonstration : L’existence et l’unicité se montrent par récurrence sur n .

Existence : Si $n = 2$, $(p_1, \alpha_1) = (2, 1)$. Si $n > 2$, n possède au moins un diviseur premier p d’après le lemme 1, et l’on peut écrire $n = pm$, avec $m < n$. Si $m = 1$, c’est fini. Sinon on applique l’hypothèse de récurrence à m pour obtenir une décomposition de m , et donc de n .

Unicité : Elle est acquise si $n = 2$ puisque $2 = q_1^{\beta_1} \dots q_m^{\beta_m}$ montre que q_i divise 2 pour tout i , autrement dit $m = 1$, $q_1 = 2$ et $\beta_1 = 1$. Supposons que l’unicité soit démontrée jusqu’au rang n , et considérons les écritures

$$n + 1 = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_m^{\beta_m},$$

avec $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_m \in \mathbb{N}^*$, et où les $p_1, \dots, p_k, q_1, \dots, q_m \in \mathbb{N}$ sont premiers. p_k divise $q_1^{\beta_1} \dots q_m^{\beta_m}$, donc divisera l’un des q_i d’après le lemme 3, par exemple $p_k | q_m$. Comme p_k est premier, cela entraîne $p_k = q_m$ et

$$\frac{n + 1}{p_k} = p_1^{\alpha_1} \dots p_k^{\alpha_k - 1} = q_1^{\beta_1} \dots q_m^{\beta_m - 1}.$$

On applique l’hypothèse de récurrence à cette décomposition en distinguant deux cas pour que les exposants soient tous strictement positifs : si $\alpha_k = 1$, alors $\beta_m = 1$, autrement q_m diviserait l’un des p_i avec $i \neq k$, absurde. Si $\alpha_k > 1$, alors $\beta_m > 1$, autrement p_k diviserait l’un des q_i avec $i \neq m$, ce qui est absurde.

Ces récurrence terminent cette démonstration. ■

Corollaire : Si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, alors n admet $\prod_{i=1}^n (1 + \alpha_i)$ diviseurs.

démonstration : Les diviseurs de n sont tous les termes du développement du produit $\prod_{k=1}^n (1 + p_k + \dots + p_k^{\alpha_k})$. Leur nombre est donc $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_n) = \prod_{i=1}^n (1 + \alpha_i)$. ■

13.3 Recherche des nombres premiers

Proposition 2 : Un nombre $n \in \mathbb{N} \setminus \{0, 1\}$ est premier si et seulement s'il n'admet pas de diviseur différent de 1 et tel que $d^2 > n$.

démonstration :

\Rightarrow : Si n admet un diviseur $d \neq 1$ tel que $d^2 \leq n$, alors $1 < d < n$ et n n'est pas premier.

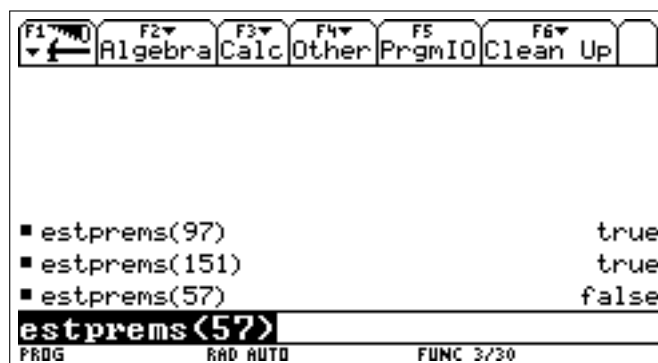
\Leftarrow : Si n n'est pas premier, n s'écrit $n = dq$ avec $1 < d \leq q$, et donc $d^2 \leq dq \Leftrightarrow d^2 \leq n$.

■

Remarques :

- Ce lemme est encore vrai si l'on remplace d par un « diviseur premier p tel que $p^2 \leq n$ », comme on le démontre en modifiant légèrement la démonstration : on choisit un diviseur premier p de d au lieu de d lui-même, et l'on obtient encore $p^2 \leq d^2 \leq dq = n$.
- Ce lemme est utilisé comme test d'arrêt, même pour un calcul « à la main » : pour savoir si 97 est premier ou non, on vérifie s'il est divisible par 2, 3, 5, 7, 11 et l'on s'arrête puisque $11^2 > 97$. Aucune des divisions ne tombe juste, donc 97 est premier.
- C'est aussi le critère d'arrêt dans le programme suivant permettant de savoir si un nombre donné est premier ou pas. Dans ce programme, on se donne un entier naturel n différent de 0 et 1, puis on le divise successivement par tous les entiers d supérieurs à 2 et tels que $d^2 \leq n$. Si l'une des divisions tombe juste, n n'est pas premier, autrement il l'est. En fait, on vérifie dès le début si n est pair ou non, pour ensuite n'envisager que les divisibilités par des nombres impairs, ce qui fait gagner du temps de calcul. Le programme est donné pour TI Voyage 200.

```
estprems(n)
Func
Local i
For i,2,int(n^(1/2))
  If int(n/i)=n/i Then
    Return false
  EndIf
EndFor
Return true
EndFunc
```



En tapant `estprems(97)`, la calculatrice renvoie `true`, et si l'on essaie la fonction sur un nombre non premier, elle renverra `false`. Le fait qu'elle renvoie un booléen permet à un autre programme d'en utiliser le résultat.

13.3.1 Crible d'Eratosthène

1	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
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

C'est la table de \mathbb{N} , par exemple de 1 à 100. On entoure 2 et raye ses multiples, puis on entoure 3 et raye ses multiples, . . . , et enfin on entoure 10 et raye ses multiples. Tous les nombres entourés sont donc premiers.

En effet, pour $p \in \mathbb{N}$, on montre que le premier nombre à rayer est p^2 . En effet, tous ceux qui le précèdent sont de la forme αp ($\alpha < p$) et ont été rayés comme multiples de α si α est premier, ou comme multiples de l'un des diviseurs premiers de α . On se permet donc d'arrêter de rayer les entiers de ce tableau dès qu'on est arrivé à 10.

13.4 Remarques générales et compléments

Remarques :

- 0 et 1 ne sont pas premiers.
- Il est souvent intéressant de définir ce qu'est un nombre premier dans \mathbb{Z} : un entier relatif est dit *premier* s'il est distinct de ± 1 et n'admet pas d'autres diviseurs (dans \mathbb{Z}) que les diviseurs triviaux ± 1 et $\pm n$, mais cela n'est pas indispensable. Connaître les nombres premiers dans \mathbb{N} revient à connaître les nombres premiers dans \mathbb{Z} puisque $n \in \mathbb{Z}$ est premier si et seulement si $|n|$ est premier dans \mathbb{N} . Dans cet exposé, nous nous sommes volontairement placé, autant que possible, dans \mathbb{N} .
- On appelle *nombre de Fermat* tout nombre de la forme $F_t = 2^{2^t} + 1$ avec $t \in \mathbb{N}$. Le calcul de F_t pour des petites valeurs de t fournit les nombres premiers :

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537,$$

et Fermat conjectura un peu vite que la propriété pourrait être vraie pour absolument tous les nombres F_t . En 1733, Euler montra qu'il n'en était rien en proposant une factorisation du cinquième nombre de Fermat :

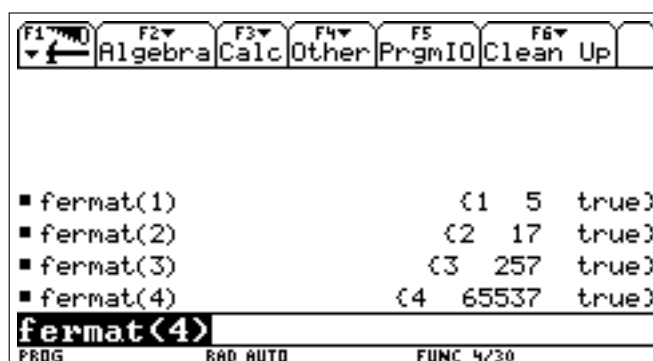
$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

Si la factorisation de F_5 est aujourd'hui facile à trouver à l'aide d'une calculatrice, on eût imaginé combien elle devait être difficile à obtenir à l'époque d'Euler. On sait aujourd'hui que les nombres F_5 à F_{30} sont composés, et l'on a encore trouvé que très peu de nombres premiers de Fermat.

Nombre premiers, décomposition en facteurs premiers

[Idée : écrire un petit programme qui calcule les premiers nombres de Fermat et vérifie s'ils sont premiers ou non, et présenter la sortie écran à l'aide de la tablette de rétroprojection. Sur TI Voyage 200, on peut écrire :

```
fermat(n)
Func
  Local f, l1, t
  {n} → l1
  2^(2^n)+1 → f
  augment(l1, {f}) → l1
  maths\estprems(f) → t
  augment(l1, {t}) → l1
  Return l1
EndFunc
```



La fonction `estprems` a été définie précédemment. Pour la sortie, il suffira alors de taper dans l'écran « home » `fermat(3)` pour obtenir le résultat suivant : {3 257 true}.

- Un nombre de Mersenne est un entier de la forme $M_n = 2^n - 1$. Certains nombres de Mersenne sont premiers, mais pas tous :

$$M_2 = 3, \quad M_3 = 7, \quad M_4 = 15, \quad M_5 = 31.$$

On démontre facilement que si $a_n - 1$ est premier ($a \geq 2$ et $n \geq 2$), alors $a = 2$ et n est premier, mais la réciproque est fautive. On ne sait toujours pas si l'ensemble des nombres premiers de Mersenne est infini.

Petit théorème de Fermat : Pour tous $n \in \mathbb{N}^*$ et $p \in \mathbb{N}^*$ premier, $n^p - n$ est divisible par p , et si de plus p ne divise pas n , alors p divise $n^{p-1} - 1$.

démonstration : Soient p premier et $k < p$. On montre que $k! \wedge p = 1$, et l'on en déduit que $\binom{p}{k} = \lambda p$ ($\lambda \in \mathbb{N}$), donc $\binom{p}{k} \equiv 0 [p]$, d'où pour tout $a_i \in \mathbb{N}$, $(a_1 + \dots + a_n)^p \equiv a_1^p + \dots + a_n^p [p]$ et conclure en faisant $a_i = 1$ pour tout i . ■

Théorème de Wilson : Soit $p \in \mathbb{N}^*$. Alors $p \mid (p-1)! + 1 \Leftrightarrow p$ premier.

démonstration : Supposons que $p = dq$ ($1 \leq d \leq q$). $d \mid p$ donc $d \mid (p-1)! + 1$. Mais d étant l'un des facteurs de $(p-1)!$, $d \mid (p-1)!$ et donc $d \mid 1$, ce qui est absurde. Réciproquement, le théorème précédent implique que pour tout $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$, $\bar{a}^{p-1} = \bar{1}$. En poursuivant ce calcul, on aboutit à $(p-1)! + \bar{1} = \bar{0}$, donc $(p-1)! + 1 \equiv 0 [p]$. ■