ARITHMETIQUE ET MATRICE :

Nombres premiers

Table des matières

Première partie: Arithmétique

Chapitre III : Nombres premiers

Les entiers 2q sont les entiers pairs et les entiers 2q + 1 sont les entiers impairs.

I. Théorème

Soit a et b deux entiers relatifs tels que b≠0. Il existe un unique couple (q,r) élément de $\mathbb{Z}\times\mathbb{N}$ tel que :

a=bq+r et 0≤r <|b|.

Les nombres q et r s'appellent respectivement le quotient et le reste de la division euclidienne de a par b. Effectuer une division euclidienne c'est déterminer son reste et son quotient.

II. Démonstration

1. Existence

Soit A l'ensemble des entiers naturels de la forme : a−bq (q $\in\mathbb{Z}$). A n'est pas vide car a+|ba|est élément de A.

A est une partie non vide de N, donc A admet un plus petit élément r

On a: r ∈A et A∈N; donc: 0≤r. Il existe un entier relatif q tel que : r =a−bq. On a : r −|b|=a−bq−|b|; donc il existe un entier relatif q′ tel que : r −|b|=a−bq′. r est le plus petit élément de A et : r −|b|<r ; donc: r −|b|∉A; d'où: r −|b|<0.

Il existe donc un couple (q,r)tel que : a=bq+r et 0≤ r <|b|.

2. Unicité

Soit (q,r)et (q′,r′)deux couples tels que : a=bq+r ; a=bq′+r′; 0≤r <|b|et 0≤r′<|b|.

On a:$0=b(q'-q)+r'-r$; donc :$|r'-r|=|b||q'-q|$. Or : $0 \leq r'<|b|$et$-|b|<-r \leq 0$; donc : $-|b|<r'-r<|b|$; d'où :$|r'-r|<|b|$; c'est-à-dire:$|b||q'-q|<|b|$.

De plus :$|b| \neq 0$; donc par quotient :$|q'-q|<1$; d'où :$|q'-q|=0$; c'est-à-dire: $q'=q$.

De plus : $r'=a-bq'=a-bq=r$.

Le couple (q,r)est donc unique.

Exemples

a=47et b=9

On a :$47=9\times5+2$ et $0\leq2<9$.

Donc : q =5 et r =2.

a=47et b=−9

On a :$47=(-9)\times(-5)+2$ et $0\leq2<9$.

Donc : q =−5et r =2.

a=-47et b=9

On a : $-47=(-9)\times(5)+2$ ou $9x(-5)+2$ et $0\leq2<9$.

Donc : q = +/- 5 et r = 2.

III. Théorème 1

Soit a, b et n trois entiers relatifs. Si a et b sont multiples de n alors, pour tous entiers u et v, au+bv est multiple de n.

Démonstration

On a : $a=a'n$ et $b=b'n$ (avec $a' \in Z$ et $b' \in Z$); donc: $au+bv=(a'u+b'v)n$

1. Définition

Un nombre premier p est un entier naturel qui possède exactement deux diviseurs positifs : 1et p.

Exemples

1. **Les six premiers nombres premiers** sont :**2 ;3 ;5 ;7 ;11 ;13**.
2. **6 et121 ne sont pas des nombres premiers** car :6=2×3 et 121=11×11.

Remarques

1. 0 et1 ne sont pas des nombres premiers.
2. Deux nombres premiers distincts sont premiers entre eux (car 1 est le diviseur commun positif).

2. Théorème 2

Tout entier naturel $n \geq 2$ admet au moins un diviseur premier.

Démonstration

Soit A l'ensemble des diviseurs de n supérieurs ou égaux à 2 :

$A = \{d \geq 2 | d \in D(n)\}$.

On a : $n \in A$; donc A n'est pas vide, par conséquent il admet un plus petit élément p. Si p était composé il admettrait un diviseur propre positif p′ qui serait à la fois élément de A et strictement plus petit que le plus petit élément de A, ce qui est contradictoire ; donc p est un nombre premier et puisque $p \in A$, p est un diviseur de n.

Remarque :

L'ensemble des diviseurs premiers de n n'est pas vide, il admet donc un plus petit élément : le plus petit diviseur premier de n.

3. Reconnaitre un nombre premier

a) Teste de primalité

Soit n un entier naturel ($n \geq 2$). Si n n'est pas premier alors il admet au moins un diviseur d tel que :$2 \leq d^2 \leq n$.

Démonstration

Si n n'est pas premier, il admet au moins un diviseur entier naturel autre que 1 et n. Il existe donc deux entiers naturels d et d′ tels que : n =d × d′ et 2≤d ≤ d′. On a donc : 2≤d ; et en multipliant la seconde inégalité membre à membre par d on obtient : $d^2 \leq n$.

Remarques

1. D'après le théorème, d admet un diviseur premier p et on a donc : $p^2 \leq n$; c'est-à-dire : $p \leq \sqrt{n}$.

2. En pratique c'est la contraposée de cette dernière implication qui est utilisée : «si n n'a aucun diviseur premier, p, tel que : $p \leq \sqrt{n}$; alors n est premier ».

Exemple :113 et 437 sont-ils premiers ?

$\sqrt{113} \approx 10{,}63$

2 ; 3 ; 5 ; 7 sont les nombres premiers inférieur à 10

113 n'est pas divisible par 2 ; 3 ;5 ;7**.**

Donc 113 est premier

$\sqrt{437} \approx 20{,}90$

2 ; 3 ; 5 ; 7 ;11 ;13 ;17 ;19 sont les nombres premiers inférieur à 20

437=19x23, **donc 437 n'est pas un nombre premier**

b) Le crible d'Eratosthène

Un nombre est dit premier, s'il admet exactement deux diviseurs distincts (lui-même et l'unité). 1 n'est donc pas premier.

On désigne sous le nom de crible d'Eratosthène, une méthode de recherche des nombres premiers plus petit qu'un entier naturel n donné.

Pour ceci, on écrit la liste de tous les nombres jusqu'à 127.

On élimine 1

On prend 2 et on élimine tous les multiples de 2

Puis, on fait de même avec 3.

On choisit après le plus petit nombre non éliminé et non pris (ici c'est 5) et on élimine tous ses multiples.

Les nombres non éliminés sont les nombres premiers jusqu'à 127

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
101	102	103	104	105	106	107	108	109
110	111	112	113	114	115	116	117	118
119	120	121	122	123	124	125	126	127

TAB. I.1 – Crible d'ÉRATOSTHÈNE (début)

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~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109
~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~
~~119~~	~~120~~	~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127

TAB. I.2 – Crible d'ÉRATOSTHÈNE (fin)

IV. Nombres premiers et divisibilité

1. Théorème1 :

Soit p un nombre premier et a un entier relatif. Si a n'est pas divisible par p alors a et p sont premiers entre eux.

2. Théorème2 :

Soit p un nombre premier et a, b deux entiers relatifs.

(1) Si p divise ab alors p divise a ou p divise b.

(2) Si de plus a et b sont premiers alors p =a ou p=b.

Plus généralement ce théorème s'étend, par récurrence, à un nombre quelconque de facteurs et nous obtenons alors le corollaire suivant que nous admettons :

Soit p un nombre premier et $a_1, a_2, \cdots, a_n$, n entiers relatifs(avec n≥2).

(1) Si p divise $a_1 \times a_2 \times \cdots \times a_n$ alors p divise l'un des facteurs a_i.

(2) Si de plus les facteurs a_i sont premiers alors p est l'un d'eux.

Remarque : En particulier si p divise a_n (avec $n \leq 1$) alors p divise a.

V. Décomposition en produit de facteurs premiers

Théorème fondamental de l'arithmétique

On a vu en introduction des nombres premiers que les nombres premiers peuvent servir à décomposer les autres entiers naturels en produit, par exemple :

– on a : 12=22×3 ;

– on a : 3=3(3est un nombre premier) ;

– on a : 720=24×32×5. Plus généralement, on a le théorème suivant :

Soit a un entier tel que : $a \geq 2$. Il existe un entier naturel non nul n, n nombres premiers distincts $p_1,...,p_n$ et n entiers naturels tous non nuls $\alpha_1,\cdots,\alpha_n$ tels que:

$a=p_1^{\alpha 1} \times \cdots \times p_n^{\alpha n}$ et $p_1<p_2<\cdots<p_n$.

De plus cette décomposition est unique.