Mathématiques 1S

Arithmétique

Nombres premiers

Partie II : NOMBRES PREMIERS

Objectifs d'apprentissages	**Contenus**	**Observations**
□ Convertir un nombre d'une base de numération à une autre. □ Reconnaitre si un nombre donné est premier ou non.	- Nombre premier - Divisibilité et décomposition d'un nombre en produit de facteurs premiers.	DEFINITION : Un nombre est premier s'il a exactement deux diviseurs.

I. Définition d'un nombre premier

On dit qu'un entier naturel p est un nombre premier si p admet exactement deux diviseurs positifs distincts : 1 et p.

Un entier n 2 qui n'est pas premier est dit composé.

Exemples :

- La liste des nombres premiers nombres premiers inférieurs à 20 est : 2 ; 3 ; 5 ; 7 ; 11 ;1 3; 19.
- Les nombres 4 = 2x2 ; 6 = 2x3 ; et 15 = 3x5 sont composés.

Remarques

1. Le nombres 0 n'est pas premier car il admet une infinité de diviseurs positifs (tout entier naturel divise zéro).
2. Le nombre 1 n'est pas premier car il possède un seul diviseur positif (lui-même).
3. Ainsi, les nombres 0 et 1 ne sont ni premiers ni composés. En revanche, tout entier $n \geq 2$ est soit premier soit composé.
4. Le nombre 2 est le seul nombre premier pair car si n est un nombre pair supérieur ou égal à 4 alors n admet au moins 3 diviseur positifs distincts : 1 ; 2 et n.
5. Deux nombres premiers distincts sont premiers entre eux (car 1 est le diviseur commun positif).

Application 1: Soit $n \in N$ et An = n2 +4n+3. Déterminer, en fonction de n, si n est premier ou composé.

II. Primalité d'un entier

Tout entier $n \geq 2$ admet au moins un diviseur premier. Si **n n'est pas premier**, alors il admet un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$

Démonstrations

Soit $n \geq 2$

-Cas où n est premier ***:*** *Il admet donc bien un diviseur premier : lui-même.*

-Cas où n n'est pas premier :

*Soit un entier $n \geq 2$. Comme $n > 1$, l'ensemble $D_+(n)$ des diviseurs **d** > 1 de n est non vide (il contient au moins n). Notons p le plus petit élément de $D_+(n)$. Si p n'est pas premier, il admet un diviseur positif **d** autre que 1 et p. Ainsi, $1 < d < p$. Or, **d** divise p et p divise n donc, par transitivité de la divisibilité, **d** divise n. C'est absurde par minimalité de p. Ainsi, p est premier.*

III. Reconnaitre un nombre premier

1. Méthode des divisions successives

La primalité d'un entier montre donc que, pour tester si un entier est premier, il suffit de tester s'il admet des diviseurs premiers inférieurs ou égal à la partie entière de sa racine carrée.

Exemple. Le nombre 131 est-il premier ?

Solution :

Comme la partie entière de la racine de 131 est 11, $E(\sqrt{131}) = 11$, il suffit de tester si 131 est divisible par 2, 3, 5, 7 et 11.

Comme 131 est impair, il n'est pas divisible par 2.

Comme $1 + 3 + 1 = 5$, il n'est pas divisible par 3.

Comme son dernier chiffre est 1, il n'est pas divisible par 5

Comme $1 - 3 + 1 = -1$, il n'est pas divisible par 11.

Reste à tester la divisibilité par 7. Or, $131 = 7 \times 18 + 5$ donc 131 n'est pas divisible par 7.

On conclut donc que 131 est un nombre premier.

2. Méthode du crible d'Ératosthène

Pour déterminer les nombres premiers compris entre 2 et n, il suffit d'éliminer tous les multiples stricts des nombres premiers compris entre 2 et E(√n). Cela constitue ce qu'on appelle la méthode du crible d'Ératosthène.

Mettons-la en œuvre pour déterminer les nombres premiers inférieurs ou égaux à 100.

Comment √100 = 10, il suffit d'éliminer tous les diviseurs stricts des nombres premiers inférieurs à 10 c'est à dire 2, 3, 5 et 7.

On commence par barrer tous les multiples stricts de 2 puis de 3 non encore barrés ensuite les multiples stricts de 5 et en fin les multiples stricts de 7 :

	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~~

	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~~

	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~~

	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~~

Les nombres qui ne sont pas barrés sont exactement les nombres premiers inférieurs ou égaux à 100 :

	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~~

Il y en a 25. En voici la liste : 2; 3; 5; 7; 11; 13; 17; 19; 23; 29; 31; 37; 41; 43; 47; 53; 59; 61; 67; 71; 73; 79; 83; 89 et 97.

IV. Divisibilité et décomposition en produit de facteurs premiers

1. Divisibilité-division euclidienne

Soit a et b deux entiers relatifs.

a *divise* b si et seulement si b peut s'écrire $b=k.a$ où $k \in Z$

On dit aussi que

- a est un *diviseur* de b
- b est *divisible* par a
- b est un *multiple* de a

Exemple : 63 est divisible par 9 car $-63=9\times(-7)$

Tout nombre entier relatif divise 0 puisque $\forall a \in Z$: $a\times 0=0$

Remarque : Tout entier relatif possède un nombre fini de diviseur

En effet, si a *divise* b, $|a|<|b|$. Il n'y a donc qu'un nombre fini de diviseurs potentiels.

Application 2 : n désigne un entier naturel. Démontrer que $n-1$ divise n^2+3n-4

2. Propriété de la divisibilité

Soit a, b et c 3 entiers relatifs.
Si a divise b et b divise c, alors a divise c

Démonstration : a divise b donc il existe en entier $q1$ tel que $b = q_1.a$
b divise c donc il existe en entier q_2 tel que $c = q_2.b$
Donc $c = q_2.b = q_2.q_1.a$. Puisque $q_2.q_1$ est entier, a divise c.

3. Combinaison linéaire

Soit a, b et c 3 entiers relatifs.
Si a divise b et c, alors a divise toute combinaison linéaire de b et c, c'est-à-dire pour tout entier u et v, a divise $bu+cv$

Exemple : Soit n un entier naturel.
Montrer que seuls 1 ou 7 peuvent diviser à la fois $n-3$ et $2n+1$

Solution : Si un entier divise 2 nombres, il divise toute combinaison linéaire de ces nombres.

Soit a un entier naturel divisant à la fois $n-3$ et $2n+1$. Il divise donc $(2n+1)-2\times(n-3)=7$

Or 7 n'est divisible que par 1 ou 7. Donc, seuls 1 et 7 peuvent diviser à la fois n-3 et 2n+1

Application 3 : Déterminer les nombres entiers relatifs n tels que $n-1$ divise $n+5$

4. Propriété et définition de la division euclidienne

Soit a un entier relatif et b un entier naturel non nul.

Il existe un couple unique d'entiers $(q\ ;\ r)$ tels que $a = bq+r$ avec $0 \leqslant r < b$

- a est le *dividende*
- b est le *diviseur*
- q est le *quotient* de la division euclidienne de a par b
- r est le *reste*.

Démonstration de l'unicité :

On suppose qu'il existe deux couples $(q\ ;\ r)$ et $(q'\ ;\ r')$. Vérifiant $a=bq+r=bq'+r'$.

On a donc : $b(q-q') = r'-r$.

Puisque $q-q'$ est entier, $r'-r$ est un multiple de b.

Or on sait que $0 \leqslant r' < b'$

De même $0 \leqslant r < b$ ce qui équivaut à $-b < -r \leqslant 0$

En ajoutant ces deux inégalités on obtient l'encadrement

$-b < r'-r < b$ Mais le seul multiple de b strictement compris entre $-b$ et b est 0

Donc $r'-r=0$ soit $r=r'$

Et puisque $b(q-q') = r'-r=0$ et que b est non nul, c'est que $q=q'$.

Cela prouve l'unicité.

Démonstration de l'existence :

On distingue 2 cas

Premier cas : a est un multiple de b

Donc $a=qb=qb+0$ ce qui prouve l'existence d'une forme du type $a=bq+r$ avec $r=0$.

Second cas : a n'est pas un multiple de b

La suite des multiples de b est : … ; $-kb$;$(-k-1)\ b$… ; $-b$;0 ; b ;$2b$… ; kb;$(k+1)\ b$; …

Dans le cas où a n'est pas un multiple de b, il existe des entiers de la suite des multiples de b qui sont inférieurs à a, et d'autres qui sont supérieurs à a. Ce dernier va donc se trouver encadré par deux termes consécutifs de la suite : $\ldots < (q-1)\ b < qb < a < (q+1)\ b < \ldots$

On définit ainsi un entier q tel que qb et $(q+1)\ b$ encadrent a : $qb < a < (q+1)\ b \Leftrightarrow 0 < a-qb < b$

Posons alors $r=a-qb$, on a alors $0<r<b$

Conclusion :

En faisant le bilan des deux cas, on a bien $a=bq+r$ avec $0 \leqslant r < b$, le cas $r=0$ correspondant au cas où b divise a.

5. Théorème fondamental de l’arithmétique

Tout entier $n \geq 2$ peut s’écrire comme un produit de nombres premiers (éventuellement réduit à un seul facteur).

La décomposition en produit de facteurs premiers consiste à écrire un entier strictement positif sous forme d'un produit de nombres premiers. Cette factorisation est unique et existe pour tous les nombre.