BTS SIO – 1

Chapitre IV

Arithmétique - 2

Contenus

- Nombres premiers, décomposition en produit de facteurs premiers, entiers premiers entre eux, PGCD de deux entiers.

Capacités

- Décomposer un entier naturel en produit de facteurs premiers et déterminer tous ses diviseurs.
- Mettre en œuvre un algorithme :
  - de recherche de nombres premiers ;
  - de décomposition en produit de facteurs premiers.

Table des matières

I. Nombres premiers

Les nombres premiers jouent un rôle crucial, notamment en cryptographie. Par exemple, le système de cryptage RSA, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet (protocoles d'identification SSL (Secure Sockets Layer), etc), repose sur les nombres premiers. Plus les nombres premiers utilisés pour le cryptage sont grands, plus le cryptage est sûr.
C'est pour cela qu'on s'intéresse aux méthodes permettant d'identifier les nombres premiers.

I.1. Définition

Un nombre premier est un entier naturel qui admet exactement deux diviseurs distincts positifs : 1 et lui même.

Exemples

- 1 .....
- 2 .....
- 6 .....

Liste des nombres premiers inférieurs à 20 : .....

Remarque : Il existe une infinité de nombres premiers.

I.2. Recherche de nombres premiers

Méthode par essais de division :
La méthode repose sur le théorème suivant :

Théorème
a) Tout entier naturel n ≥ 2 admet au moins un diviseur premier.
b) Si n n'est pas premier, alors il admet un diviseur p premier tel que : $2 \leq p \leq \sqrt{n}$.

Conséquence :
Pour savoir si un nombre est premier, on regarde s'il est divisible par un nombre premier inférieur ou égal à sa racine. S'il n'est divisible par aucun de ces nombres, il est premier.

Exemple

- 133 est-il premier ?

- 241 est-il premier ?

Méthode : Le crible d'Ératosthène

Le crible d'Ératosthène repose sur la même idée que la méthode ci-dessus et permet de déterminer la liste des premiers nombres premiers.

Exemple :
On souhaite déterminer tous les nombres premiers inférieurs à 50 :

		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

I.3. Décomposition en produit de facteurs premiers

Théorème - Définition
Tout nombre entier $n \geq 2$ peut s'écrire comme un produit de nombres premiers :

$$n = {p_1}^{n_1} \times {p_2}^{n_2} \ldots \times {p_k}^{k} ,$$

où les p_i sont tous premiers, et où les n_i sont des entiers positifs.
Cette écriture s'appelle la décomposition en produit de facteurs premiers.

Exemple-Méthode

- Donnons la décomposition en produit de facteurs premiers de 56 :

56	2

Donnons la décomposition en produit de facteurs premiers de 550 :

II. Congruence

II.1. Définition

Soit n un entier naturel non nul. On dit que deux entiers naturels a et b sont congrus modulo n si et seulement si a et b ont le même reste dans la division euclidienne par n.
On écrit alors : $a \equiv b[n]$ *ou* $b \equiv a[n]$

Exemples :

- $21 \equiv 16[5]$
- $13 \equiv$ _____$[3]$
- $16 \equiv$ _____$[5]$
- Pour tout entier naturel a, $a \equiv 0[2]$ si et seulement si a est .....

II.2. Propriétés

- Pour tout entier naturel a et tout entier naturel $n \geq 2$, on a que :
  $a \equiv 0[n]$ si et seulement si a est multiple de n.

- Soient a et b deux entiers naturels tels que $a > b$, et n un entier naturel non nul.
  a est congru à b modulo n si et seulement si $a - b$ est un multiple de n.

- Soient a, b, c et d des entiers naturels et n un entier naturel non nul.

Si $a \equiv b[n]$ *et* $c \equiv d[n]$ alors :

- $a + c \equiv b + d[n]$
- $a - c \equiv b - d[n]$
- $pa \equiv pb[n]$ pour tout entier naturel p
- $a \times c \equiv b \times d[n]$
- $a^p \equiv b^p[n]$ pour tout entier naturel p

Exemples :

On a : $26 \equiv 10[4]$ *et* $17 \equiv 5[4]$ donc :

- $43 \equiv 15[4]$
- $9 \equiv 5[4]$
- $52 \equiv 20[4]$
- $442 \equiv 50[4]$

- sans utiliser de calculatrice, montrer que $15^3 - 3^5$ est un multiple de 12.

Exercice 1.
Quel est le plus petit nombre non nul divisible par deux nombres premiers distincts ?

Exercice 2.
Les nombres suivants sont-ils premiers ?
a) 97 b) 259 c) 143 d) 119 e) 149 f) 209

Exercice 3.
Donner la décomposition en produit de facteurs premiers des nombres suivants :
a) 16 940 b) 1 547 c) 62 181

Exercice 4.
a) Décomposer en produit de facteurs premiers les nombres suivants : 160, 126.
b) Donner les diviseurs de 126.
c) Calculer PGCD(160,12).

Exercice 5.
Donner la liste des diviseurs positifs des nombres suivants :
a) 2 093 b) 770 c) 60

Exercice 6.
a. Vérifier que $90 \equiv 6[7]$ et que $66 \equiv 3[7]$.
b. En utilisant les propriétés des congruences, compléter les résultats suivant en mettant l'entier naturel le plus petit possible :

$$90 + 66 \equiv \_\_\_\_\_[7]$$
$$4 \times 90 \equiv \_\_\_\_\_[7]$$
$$90 \times 66 \equiv \_\_\_\_\_[7]$$
$$90^2 \equiv \_\_\_\_\_[7]$$
$$66^3 \equiv \_\_\_\_\_[7]$$

Exercice 7.
a. Remplir le tableau suivant avec des entiers les plus petits possibles.

$n \equiv \_\_\_[5]$	**0**	**1**	**2**	**3**	**4**
$n^2 \equiv \_\_\_[5]$					
$n^3 \equiv \_\_\_[5]$					
$n^5 \equiv \_\_\_[5]$					
$4n \equiv \_\_\_[5]$					
$n^2 + 4n \equiv \_\_\_[5]$					

b. Interpréter la dernière ligne du tableau à l'aide d'une phrase concernant le reste d'une division euclidienne de $n^2 + 4n$.

Exercice 8.

Soit $E = \{1; 2; 3; 4; 5; 6\}$.

a. Vérifier que pour chaque élément a de E, il existe un élément b de E tel que $ab \equiv 1[7]$.

On dit que b est l'inverse de a modulo 7.

b. Résoudre l'équation $3x \equiv 4[7]$. Donner l'ensemble des solutions comprises entre 100 et 140.

Exercice 9.

Démontrer que $13^8 - 6^8$est divisible par 7.

Exercice 10.

Démontrer quel reste de la division euclidienne de 217^{30} par 7 est 0.

Exercice 11.

a. Expliquer pourquoi tout entier naturel est congru à 0, à 1, à 2, à 3, à 4 ou à 5 modulo 6.

b. Remplir le tableau suivant avec des entiers les plus petits possibles.

$n \equiv$ ___[6]	0	1	2	3	4	5
$n + 1 \equiv$ ___[6]						
$n + 2 \equiv$ ___[6]						
$n(n + 1)(n + 2) \equiv$ ___[6]						

c. Que peut-on en conclure au sujet du produit de 3 entiers consécutifs ?

Codage affine

Le chiffrement affine est une méthode simple de codage d'un message. À chaque lettre de l'alphabet, on commence par associer son rang dans l'alphabet, diminué de 1, comme l'indique le tableau ci-dessous. On obtient en entier x entre 0 et 25.

Lettre	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Nombre	0	1	2	3	4	5	6	7	8	9	10	11	12
Lettre	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Nombre	13	14	15	16	17	18	19	20	21	22	23	24	25

Le codage affine nécessite deux clés a et b, qui sont des entiers naturels compris entre 0 et 25.
On calcule alors le reste de $ax + b$ dans la division euclidienne par 26.
On obtient un entier y telles que $y \equiv ax + b\ [26]$.
On cherche à quelle lettre correspond cet entier y. Cette lettre code alors la lettre de départ.

Partie A

Dans cette partie, on choisit les clés a=3 et b=11. La fonction de codage est donc $y \equiv 3x + 11\ [26]$.
1. Montrer que G est codé par D. Comment est codé S ?
2. Remplir le tableau suivant :

Lettre	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
x	0	1	2	3	4	5	6	7	8	9	10	11	12
y							3						
Codage							D						
Lettre	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
x	13	14	15	16	17	18	19	20	21	22	23	24	25
y													
Codage													

3. Quel mot est codé par VBUTSB ?
4. On va maintenant chercher la fonction de décodage, c'est-à-dire l'expression de x en fonction de y. Cherchez l'inverse de trois modulo 26 (*cf. exercice 8*), c'est-à-dire le nombre entier cas tel que $0 \leq k \leq 25$ et $3k \equiv 1\ [26]$. En déduire la fonction de décodage.

Partie B

Dans cette partie, on choisit *a=7* et *b=12*.
1. Comment va-t-on coder le mot AFFINE ?
2. Déterminer la fonction de décodage.
3. Décoder le message CBMNJ QISO.