Arithmétique

BTS SIO

Table des matières

I Divisibilité des entiers 2
1 Multiples et diviseurs 2
2 Division euclidienne 2
II pgcd de deux nombres 3
1 Définition 3
2 Calcul du *pgcd* de deux nombres 3
2.1 Algorithme des différences 3
2.2 Algorithme d'Euclide 4
III Nombres premiers 4
IV Congruences 5

I Divisibilité des entiers

1 Multiples et diviseurs

Définition: *On dit que a est un multiple de b, ou que b est un diviseur de a lorsqu'il existe un entier k tel que $a = kb$.*

Par exemple, 60 est un multiple de 5, ou 5 est un diviseur de 60, car $60 = 12 \times 5$
Remarque : Tout entier a a au moins deux diviseurs, 1 et a.

Exercice 1

a) Donner tous les diviseurs de 12.

b) Donner tous les diviseurs de 30.

c) Combien de multiples de 8 existe-t-il entre 1000 et 2000 ?

2 Division euclidienne

Propriété: *Pour tous entiers $a$et b il existe un unique couple $(q;r)$ d'entiers tels que $a = bq + r$ et $0 \leqslant r < b$.*
q est le quotient et r le reste dans la division euclidienne de a par b.

On peut pour poser la division euclidienne, par exemple la division euclidienne de $a = 34$ par $b = 4$:

$$\begin{array}{r|l} 35 & 4 \\ \cline{2-2} -32 & 8 \\ \cline{1-1} 3 & \end{array}$$

ce qui signifie que $35 = 4 \times 8 + 3$.
Dans ce calcul,
- $a = 35$ est le **dividende**
- $b = 4$ est le **diviseur**
- $q = 8$ est le **quotient**
- $r = 3$ est le **reste**, avec $0 \leqslant r < q$

Autre exemple :

$$\begin{array}{r|l} 527 & 4 \\ \cline{2-2} -4 & 131 \\ \cline{1-1} 12 & \\ -12 & \\ \cline{1-1} 07 & \\ -4 & \\ \cline{1-1} 3 & \end{array}$$

et on a donc $527 = 4 \times 131 + 3$.

Exercice 2

Écrire la division euclidienne de 99 par 5, de 1076 par 10, de 111 par 37, de 14523 par 23.

Exercice 3

On considère les nombres $x_1 = 1$, $x_2 = 2$, $x_3 = 111$, …, $x_8 = 11\,111\,111$.

a) Trouver deux nombres parmi ces huit nombres qui ont le même reste dans la division euclidienne par 7.

b) Justifier que la différence des deux nombres trouvés, $x_p - x_q$, est un multiple de 7.

c) En déduire l'existence d'un multiple de 7 qui ne s'écrit qu'avec des 0 et des 1.

II pgcd de deux nombres

1 Définition

Étant donnés deux nombres entiers a et b, on peut écrire la liste de leurs diviseurs communs.
Par exemple, l'ensemble des diviseurs de $a = 70 = 2 \times 5 \times 7$ est $D_a = \left\{1; 2; 5; 7; 10; 14; 35; 70\right\}$
et l'ensemble des diviseurs de $b = 105 = 3 \times 5 \times 7$ est $D_b = \left\{1; 3; 5; 7; 15; 21; 35; 105\right\}$
L'ensemble de leurs diviseurs communs est donc $D = \left\{1; 5; 7; 35\right\}$

Définition: *On note $pgvd(a, b)$ le **Plus Grand Diviseur Commun** de a et b*

Par exemple, avec les calculs précédents, $pgcd(70, 105) = 35$

Exercice 4

a) 15 a pour diviseurs ..... 6 a pour diviseurs ..... donc $pgcd(6, 15) = \ldots$

b) 35 a pour diviseurs ..... 7 a pour diviseurs ..... donc $pgcd(6, 15) = \ldots$

c) 121 a pour diviseurs ..... 16 a pour diviseurs ..... donc $pgcd(6, 15) = \ldots$

Définition: *On dit que a et b sont **premiers entre eux** lorsque $pgcd(a, b) = 1$*

2 Calcul du *pgcd* de deux nombres

Propriété:
- $pgcd(a, b) = pgcd(b, a)$
- $pgcd(a, b) = pgcd(a - b, b)$
- $pgcd(a, b) = pgcd(b, r)$ *avec r le reste de la division euclidienne de a par b et donc, en particulier, $0 \leqslant r < b$*

2.1 Algorithme des différences

La 2ème propriété $pgcd(a, b) = pgcd(a - b, b)$ permet, par soustractions successives, de calculer le pgcd.
Par exemple, avec $a = 140$ et $b = 110$, on calcule successivement,

a	b	$a - b$	$pgcd(140, 110)$
140	110	30	$= pgcd(110, 30)$
110	30	80	$= pgcd(80, 30)$
80	30	50	$= pgcd(50, 30)$
50	30	20	$= pgcd(30, 20)$
30	20	10	$= pgcd(20, 10)$
20	10	10	$= pgcd(10, 10)$
10	10	**0**	$= 10$

Exercice 5 En appliquant l'algorithme des différences, déterminer le *pgcd* de :
1) $a = 123$ et $b = 21$ 2) $a = 516$ et $b = 156$ 3) $a = 580$ et $b = 348$ 4) $a = 296$ et $b = 703$

2.2 Algorithme d'Euclide

La 3ème propriété : $pgcd(a,b) = pgcd(b,r)$ avec r le reste de la division euclidienne de a par b, avec $0 \leqslant r < b$
fournit aussi un algorithme efficace pour calculer le pgcd de deux nombres.
Par exemple, avec $a = 140$ et $b = 110$

a	b	r	$pgcd(140,110)$
140	110	$140 = 1 \times 110 + \underline{\mathbf{30}}$	$= pgcd(110,30)$
110	30	$110 = 3 \times 30 + \underline{\mathbf{20}}$	$= pgcd(30,20)$
30	20	$30 * 1 \times 20 + \underline{\mathbf{10}}$	$= pgcd(20,10)$
20	10	$20 = 2 \times 10 + \underline{\mathbf{0}}$	$= 10$

Le *pgcd* est le dernier reste non nul.

Exercice 6 En appliquant l'algorithme d'Euclide, déterminer le *pgcd* de :
1) $a = 123$ et $b = 21$ 2) $a = 516$ et $b = 156$ 3) $a = 580$ et $b = 348$ 4) $a = 296$ et $b = 703$

Exercice 7

a) Une feuille A4 a pour dimensions 21cm et 29,7cm. Alice veur quadriller sa feuille à l'aide de carrés de mêmes dimensions et qui soient les plus gros possibles.
Quelle est la taille de ces carrés ? combien en faut-il ?

b) Un boulanger fait des pizzas sur des plaques de 140 × 168cm. Il veut découper ses pizzas en parts carrées, les plus grands possibles, sans faire de perte. Quelles doivent être les dimensions de ces carrés ?

III Nombres premiers

Définition: *Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même*

— 1 n'est pas premier car il a un seul diviseur
— 2 est premier ; c'est le seul nombre pair premier
— 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; . . .sont les premiers nombres premiers

Pour savoir si un nombre n est premier, il faut a priori chercher à le diviser par tous les nombres qui lui sont inférieurs. On peut être plus efficace :

Propriété:
— *Tout entier $n \geqslant 2$ admet au moins un diviseur premier.*
— *Si n n'est pas premier, il admet un diviseur premier p tel que $2 \leqslant p \leqslant \sqrt{n}$*

Exemple : $a = 143$ est-il premier ?
On a $\sqrt{143} \simeq 11,9$, et il suffit donc de chercher si 143 est divisible par les nombres premiers inférieurs à 11, soit 3, 5, 7, 11.
On trouve que $\dfrac{143}{11} = 13 \in \mathbb{N}$ et donc que 143 n'est pas premier.

Exercice 8 Déterminer si les nombres suivants sont premiers : 247, 337, 353, 613, 893

Exercice 9 Écrire un algorithme / programme Python, qui affiche si un nombre n donné est premier.

Propriété: ***Décomposition en facteurs premiers***
Tout nombre $n \geqslant 2$ s'écrit comme un produit de nombres premiers : $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$

Exemple : $12 = 4 \times 3 = 2^2 \times 3 = 2^2 \times 3^1$
$30 = 6 \times 5 = 2^1 \times 3^1 \times 3^1$
$36 = 6 \times 6 = 2 \times 3 \times 2 \times 3 = 2^2 \times 3^2$

Exercice 10 Donner la décomposition en facteurs premiers de : 360, 125, 48, 242, 165

Exercice 11 Mme Anomeny discute avec son facteur et lui dit :
« J'ai trois filles ; le produit de leurs âges fait 36. »
Le facteur lui répond que cela ne lui suffit pas pour connaître l'âge des trois filles.
Mme Anomeny ajoute alors : « La somme de leurs âges donne le numéro de la maison d'en face. »
Le facteur se retourne et regarde le numéro de la maison d'en face et dit : « cela ne me suffit toujours pas pour connaître leurs âges ! »
Mme Anomeny ajoute alors : « En effet, j'ai oublié de vous dire que l'ainée est blonde »
Le facteur sourit alors et donne l'âge des trois filles.
Quels âges ont les 3 filles ?

Propriété: ***Décomposition en facteurs premiers et pgcd***
À partir de la décomposition en facteurs premiers :
- *si dans les décompositions de a et b il n'y a pas de facteurs communs, alors a et b sont premiers entre eux : $pgcd(a, b) = 1$.*
- *sinon le pgcd a et b est le produit des facteurs premiers communs aux deux décompositions, avec la plus petite puissance avec laquelle elle figure dans les deux décompositions.*

Par exemple, $a = 90 = 2 \times 3^2 \times 5$ et $b = 84 = 2^2 \times 3 \times 7$, alors $pgcd(a, b) = 2 \times 3 = 6$

Exercice 12 Déterminer le *pgcd* de a et b en les décomposant en produits de facteurs premiers :
1) $a = 130$ et $b = 85$ 2) $a = 96$ et $b = 728$

IV Congruences

Définition: *On dit que les entiers a et b sont **congrus modulo** n lorsqu'ils ont le même reste dans la division euclidienne par n.*
On note alors $a \equiv b\,[n]$

Exemple : $21 \equiv 16\,[5]$ car $21 = 5 \times 4 + 1$ et $16 = 5 \times 3 + 1$, donc, on a aussi $21 \equiv 1\,[5]$ et $16 \equiv 1\,[5]$

Exercice 13 Compléter, avec le plus petit entier possible,

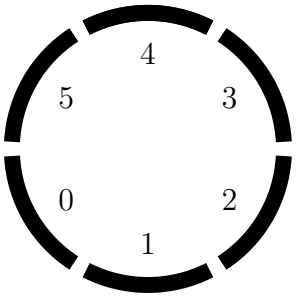
$15 \equiv \dots\,[2]$ $20 \equiv \dots\,[2]$ $147 \equiv \dots\,[2]$ $9 \equiv \dots\,[12]$ $132 \equiv \dots\,[10]$

$1634 \equiv \dots\,[10]$ $17 \equiv \dots\,[7]$ $28 \equiv \dots\,[7]$ $155 \equiv \dots\,[7]$ $623 \equiv \dots\,[3]$

A quelle condition a-t-on $p \equiv 0\,[n]$?

Propriété: *p est un multiple de n lorsque $p \equiv 0\,[n]$*

Exercice 14 Une puce se trouve initialement sur la case 0 d'un plateau circulaire de 6 cases.



a) Suposons que la puce saute par saut de 2 cases. Quelles sont les cases sur lesquelles elle va se poser ?

b) Si elle fait maintenant des sauts de 3 cases, quelles sont les cases sur lesquelles elle va se poser ?

c) Si elle fait maintenant des sauts de 8 cases, quelles sont les cases sur lesquelles elle va se poser ?

d) Et avec des sauts de 5 cases, quelles sont les cases sur lesquelles elle va se poser ?

e) Peut-elle passer par toutes les cases autrement qu'avec des sauts de 1 case ?

Remarque : le parcours du plateau de jeu, ou d'une liste, n'est exhaustif que si la longueur du saut et la taille de la liste sont premiers entre eux.

Propriété: ***Propriétés des congrences***
Si $a \equiv a'\ [n]$ *et* $b \equiv b'\ [n]$ *alors*
- $a + a' \equiv b + b'\ [n]$
- $aa' \equiv bb'\ [n]$
- $a^k \equiv a'^k\ [n]$ *pour tout enier* k.

Exemples :
— Quel est le reste de 1200 dans la division par 7 ?
On cherche donc 1200 [7] et on a

$$\begin{aligned} 1200 &= 10 \times 10 \times 12 \\ &\equiv 3 \times 3 \times 5 \ [7] \\ &\equiv 9 \times 5 \ [7] \\ &\equiv 2 \times 5 \ [7] \\ &\equiv 10 \ [7] \\ &\equiv 3 \ [7] \end{aligned}$$

— Quel est le reste de 26^{26} dans la division euclidienne par 5 ?
On a $26 = 25 \times 2 + 1$ et donc $26 \equiv 1\ [5]$, d'où $26^{26} \equiv 1^{26}\ [5]$.
Or $1^{26} = 1$ et donc $26^{26} \equiv 1\ [5]$

Exercice 15 Compléter avec l'entier nautrel le plus petit possible :

$90 \equiv \ldots\ [7]$ $\quad 66 \equiv \ldots\ [7]$

$90 + 66 \equiv \ldots\ [7]$ $\quad 8 \times 90 \equiv \ldots\ [7]$ $\quad 90 \times 66 \equiv \ldots\ [7]$ $\quad 90^2 \equiv \ldots\ [7]$

$66^3 \equiv \ldots\ [7]$ $\quad 66^4 \equiv \ldots\ [7]$ $\quad 66^5 \equiv \ldots\ [7]$ $\quad 66^{15} \equiv \ldots\ [7]$

Exercice 16

a) Quel est le chiffre des unités de 8532^{12} ?

b) Quel est le chiffre des unités de $78\,253^{20}$?

Exercice 17 Chiffrement affine

On utilise, pour simplifier ici, un alphabet de seulement 6 lettres qu'on numérote de 0 à 5.

Une méthode de chiffrement affine repose sur une fonction affine $f : x \mapsto ax + b$ avec a et b des entiers naturels. Le couple (a, b) est la clé secrète de chiffrage.

Pour coder une lettre de l'alphabet, on prend l'image de son code par f, puis le reste dans la division euclidienne par 6. On remplace alors la lettre initiale par celle qui correspond à ce reste obtenu.

Quand $a = 1$ et $b = 3$, il s'agit d'un simple décalage de 3 lettres : c'est le code qu'utilisait César.

1) On utilise la clé de chiffrage $(7, 3)$. Compléter

Lettre initiale	A	B	C	D	E	F
Code	0	1	2	3	4	5
Code chiffré						
Lettre chiffrée						

Décoder le mot chiffré : « FDCB »

2) Écrire les chiffrements de l'alphabet obtenus avec les clés $(2, 3)$, $(4, 2)$ et $(9, 1)$ dans le tableau suivant :

Alphabet	A	B	C	D	E	F
Code	0	1	2	3	4	5
Chiffrage clé $(2, 3)$						
Chiffrage clé $(4, 2)$						
Chiffrage clé $(9, 1)$						

Ces chiffrages sont-ils satisfaisants ?

Énoncer un critère sur le nombre a pour que la clé de chiffrage soit satisfaisante.

3) On utilise la clé $(35, 2)$. On chiffre donc un code x en un code y par la formule $y = f(x) \equiv 35x + 2$ [6].

Compléter avec le plus petit entier : $5 \times 35 \equiv \ldots$ [6].

En déduire une fonction affine permettant de lire un message codé : $x = g(y) = \ldots\ldots$