Thème 3	ARITHMÉTIQUE MODULAIRE (1)	Mathématiques pour l'informatique

I) La division euclidienne

Définition

La division euclidienne est l'opération qui consiste à soustraire successivement le plus grand nombre de fois possible l'entier b de l'entier a.

Exemple

Avec $a = 725$ et $b = 17$. On soustrait 17 du nombre 725 autant de fois que possible :
$725-17=708$, $708-17=691$, ... puis finalement $28-17=11$.
On a alors soustrait 42 fois de suite le nombre 17 et il nous reste 11, c'est à dire que $725-42\times17=11$ soit encore $725=42\times17+11$.
Dans cette égalité, 725 est le dividende, 17 est le diviseur, 42 est le quotient et 11 est le reste.

De façon plus générale :

Résultat important :

Soient a un entier relatif et b un entier naturel.
Il existe un unique couple $(q\ ;\ r)$ d'entiers relatifs tel que $\begin{cases} a=bq+r \\ 0\leqslant r< b \end{cases}$.
L'entier q est appelé quotient de la division euclidienne de a par b et r est appelé reste de cette division euclidienne.

II) La notion de diviseur

Définition

Si a et b sont deux entiers (relatifs), on dit que b est un diviseur de a (ou que a est divisible par b, ou encore que a est un multiple de b) et on note $b \mid a$, s'il existe un entier c tel que $a = bc$.

Exemple

$117=9\times13$ donc 9 et 13 sont deux diviseurs de 117.

Exercice 1

Remarques

1) Si $b \mid a$ alors $|b|\leqslant|a|$.
2) Si $b \mid a$ et $a \mid b$, alors $|a|=|b|$.
3) Si $b \mid a$ et $a \mid c$, alors $b \mid c$.
4) Si $b \mid a$, alors pour tout entier relatif c, $bc \mid ac$.
5) Si $c \mid a$ et $c \mid b$, alors $c \mid (au+bv)$ pour tous entiers relatifs u et v .

Exercices 2 à 5

Remarque

La relation $b \mid a$ équivaut au fait que le reste r de la division euclidienne de a par b est égal à 0.

III) La notion de nombre premier.

Définition

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

Remarques

1) 0 n'est pas premier car il admet une infinité de diviseurs.
2) 1 n'est pas premier car il n'admet qu'un seul diviseur, lui-même.
3) 2 est le seul nombre premier pair.
4) Les nombres premiers inférieurs à 100 sont : 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; 17 ; 19 ; 23 ; 29 ; 31 ; 37 ; 41 ; 43 ; 47 ; 53 ; 59 ; 61 ; 67 ; 71 ; 73 ; 79 ; 83 ; 89 ; 97.

Méthode du crible d'Ératosthène

Résultat important (dit théorème fondamental de l'arithmétique)

Tout entier naturel strictement supérieur à 1 peu-être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

Exemples

$558=2\times3\times3\times31=2\times3^2\times31$; $648=2\times2\times2\times3\times3\times3=2^3\times3^3$; $10164=2^2\times3\times7\times11^2$.

Méthode de décomposition d'un nombre en produit de facteurs premiers

Un algorithme pour décomposer un entier $n>1$ en produit de facteurs premiers peut être construit de la façon « récursive » suivante :

- si n est premier, la décomposition s'arrête ici.
- sinon :
  - trouver le plus petit nombre premier p qui divise n.
  - ajouter p à la liste des facteurs premiers et recommencer avec la valeur $\frac{n}{p}$.

On remarquera qu'il n'est pas nécessaire de tester les nombres premiers strictement supérieurs à $\sqrt{n}$ (puisque si n admettait un diviseur premier $p>\sqrt{n}$ alors on aurait $n=kp$ avec k diviseur de n vérifiant $k\leqslant\sqrt{n}$ donc un nombre déjà rencontré.

Exemple

Prenons l'exemple de $n = 6\,468$.

On écrit, dans la colonne de droite, et dans l'ordre croissant, les diviseurs premiers (2, 3, 5, etc. . .) des quotients écrits dans la colonne de gauche, jusqu'à ce que le dernier quotient obtenu soit 1 :

6468	2
3234	2
1617	3
539	7
77	7
11	11
1	

On en déduit que $6468=2\times2\times3\times7\times7\times11=2^2\times3\times7^2\times11$.

Remarque

A l'heure actuelle, il n'existe qu'un seul algorithme (appelé test de primalité AKS, découvert en 2003) permettant de déterminer avec certitude si un entier n donné est premier (et en un temps d'exécution humainement acceptable (c'est-à-dire largement inférieur à quelques milliers d'années...), en particulier, évidemment, lorsque n est très grand).
Ce type d'algorithme étant d'un niveau mathématique très largement supérieur aux compétences requises en BTS, nous nous contenterons ici de présenter le crible d'Ératosthène, qui procède par élimination des entiers non premiers (jusqu'à un certain rang N) pour donner la liste des entiers premiers inférieurs à N : on commence par faire la liste de tous les entiers naturels de 1 jusqu'à un certain entier N fixé, et on y supprime méthodiquement tous les multiples d'un entier (multiples de 2, puis multiples de 3, puis multiples de 5, etc. . .). En supprimant tous les multiples, à la fin il ne restera que les entiers qui ne sont multiples d'aucun entier, et qui sont donc les nombres premiers.

Exercices 6 et 7

IV) Plus grand diviseur commun (PGCD) et Plus petit multiple commun (PPCM)

Définition

Si a et b sont deux entiers relatifs, on appelle :

- PGCD de a et b, noté PGCD(a,b) ou $a \wedge b$ le plus grand des diviseurs communs de a et b lorsque $(a,b) \neq (0,0)$. On convient de plus que PGCD(0,0)=0.
- PPCM de a et b, noté PPCM(a,b) ou $a \vee b$ le plus petit des multiples strictement positifs de a et b lorsque $ab \neq 0$. On convient de plus que PPCM(0,0)=0.
- ON dit que plus que a et b sont premiers entre eux lorsque PGCD(a,b)=1, c'est à dire lorsque les seuls diviseurs communs sont 1 et -1.

Remarque

Si on connaît la décomposition en produit de facteurs premiers de a et b alors :

- PGCD(a,b) a une décomposition contenant chacun des facteurs contenu dans celles de a et b affecté de la plus petite des deux puissances.
- PPCM(a,b) a une décomposition contenant chacun des facteurs contenu dans celles de a et b affecté de la plus grande des deux puissances.

Exemple

Pour $a=24=2^3\times 3$ et $b=36=2^2\times 3^2$ on a : $PGCD(a,b)=2^2\times 3^1=12$ et $PPCM(a,b)=2^3\times 3^2=72$.

24	2
12	2
6	2
3	3
1	

$2^3 \times 3$

$\frac{a \times b}{PGCD} = PPCM$

Remarque

PGCD(a,b) × PPCM(a,b)=a × b.
(*On a bien :* $12\times 72=864=24\times 36$).

Exercice 9

V) Algorithme d'Euclide

L'algorithme d'Euclide est un moyen de calculer le PGCD de deux entiers par divisions euclidiennes successives. Il repose sur le constat suivant : si a et b sont deux entiers naturels (avec $b \neq 0$), dont la division euclidienne s'écrit $a = bq + r$, et si d est un diviseur commun à a et b, alors $d \mid (bq)$ et $d \mid a$, donc $d \mid (a - bq) = r$ et ainsi d est aussi un diviseur commun à b et r. Inversement, tout diviseur commun à b et r divise aussi $a = bq + r$. Par conséquent :

Si a et b sont deux entiers naturels (avec $b \neq 0$), alors $PGCD(a,b) = PGCD(b,r)$.

Comme $r < b$ on se ramène donc à un couple $(b;r)$ d'entiers plus petits. Il suffit alors de recommencer et faire la division euclidienne de b par r, et ainsi de suite jusqu'à ce qu'on obtienne un dernier reste nul. Le

PGCD de a et b est donc le reste non nul obtenu juste avant.

Exemples (calcul pratique d'un PGCD)

1. Avec $a=72$ et $b=44$, les divisions euclidiennes successives fournissent les résultats suivants (les restes sont dans la deuxième ligne) :

72	44	28	16	12	3
44	28	16	12	4	0

Le dernier reste non nul obtenu est 4, donc on a $PGCD(72,44)=4$.

2. Avec $a=120$ et $b=23$, les divisions euclidiennes successives fournissent les résultats suivants :

120	23	5	3	2	1
23	5	3	2	1	0

Le dernier reste non nul obtenu est 1, donc on a PGCD (120 ; 23) = 1 (c'est-à-dire que 261 et 203 sont premiers entre eux).

3. Avec $a=5283$ et $b=4095$, les divisions euclidiennes successives fournissent les résultats suivants :

5283	4095	1188	531	126	27	18	9
4095	1188	531	126	27	18	9	0

Le dernier reste non nul obtenu est 9, donc on a PGCD (5283 ; 4095) = 9.

Exercice 10

VI) Égalité de Bachet-Bezout

Propriété

Le *PGCD* de deux entiers a et b peut s'écrire, d'une certaine façon, comme combinaison de a et de b. C'est l'égalité de Bachet-Bezout :

Si a et b sont deux entiers (relatifs) non tous nuls, et si $d=PGCD(a;b)$ alors il existe deux entiers (relatifs) x et y tels que $xa+yb=d$.

En particulier :

a et b sont premiers entre eux si et seulement s'il existe deux entiers (relatifs) x et y tels que $xa+yb=1$.

Exemple (Algorithme d'Euclide étendu) :

La méthode ci-après, qu'on appelle l'algorithme d'Euclide étendu, permet de trouver explicitement un couple $(x;y)$ tel que $xa+yb=PGCD(a;b)$. Nous allons l'appliquer sur le cas de $a=120$ et $b=23$, en explicitant le calcul de leur *PGCD* qui a déjà été fait avec l'algorithme d'Euclide dans un exemple antérieur. Le tableau suivant donne les détails de calcul à chaque étape :

$$5=120-5\times 23=1\times 120+(-5)\times 23$$
$$3=23-4\times 5=23-4\times(1\times 120+(-5)\times 23)=(-4)\times 120+21\times 23$$
$$2=5-1\times 3=(1\times 120+(-5)\times 23)+(-1)\times((-4)\times 120+21\times 23)=5\times 120+(-26)\times 23$$
$$1=3-1\times 2=((-4)\times 120+21\times 23)+(-1)\times(5\times 120+(-26)\times 23)=(-9)\times 120+47\times 23.$$

On obtient donc : $1=(-9)\times 120+47\times 23$ d'où $a=120$, $b=23$, $x=-9$ et $y=47$.

Exercices 11 et 12

VII) Congruences

Propriété

Soit $p \geqslant 2$ un entier. On dit que l'entier a est congru modulo p à l'entier b si $a-b$ est un multiple de p et on note alors $a \equiv b\,[p]$ ou encore $a \equiv b \mod p$.

Exemples

$17 \equiv 8\ [3]$, $23 \equiv 2\ [3]$, $23 \equiv -1\ [3]$.

Remarques

- a est un multiple de b ssi $a \equiv 0\ [b]$.
- $a \equiv b\ [p]$ ssi a et b ont le même reste r dans la division euclidienne par p.
  Dans ce cas a et b sont tous deux congrus à r modulo p.

Propriétés

La relation de congruence modulo p est compatible avec les opérations algébriques usuelles :

Si $a \equiv b\ [p]$ et $c \equiv d\ [p]$

1) $a+c \equiv b+d\ [p]$
2) $ac \equiv bd\ [p]$
3) $a^k \equiv b^k\ [p]$ (pour tout entier naturel k)
4) $na \equiv nb\ [p]$ (pour tout entier relatif).

Exemple

Congruence modulo 9

Il est particulièrement simple de calculer (en base 10) le reste modulo 9 d'un entier. Il est d'abord clair que $10 \equiv 1\ [9]$, donc, pour tout entier naturel k, on a $10^k \equiv 1\ [9]$.

Soit maintenant x un entier qui s'écrit (en base 10) avec les chiffres successifs (de gauche à droite) a_n, a_{n-1},..., a_2, a_1, a_0, c'est-à-dire $x = (a_n a_{n-1} \ldots a_2 a_1 a_0)_{10}$.

Cela signifie que $x = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_2 10^2 + a_1 10^1 + a_0 10^0$ et, par conséquent, $x \equiv a_n + a_{n-1} + \ldots + a_2 + a_1 + a_0\ [9]$. Autrement dit, modulo 9, un entier est toujours congru à la somme de ses chiffres.

Par exemple, pour 1783 : 1+7+8+3 = 19, et comme $19 \equiv 1\ [9]$, on a : $1783 \equiv 1\ [9]$.

Par ailleurs, lorsqu'un nombre possède un chiffre lui-même égal à 9, il n'est pas nécessaire (puisque, évidemment, $9 \equiv 0\ [9]$) de le compter dans la somme des chiffres pour obtenir son reste modulo 9 : par exemple pour 29 597 : 2+5+7 = 14 $\equiv$ 5 [9].

Dans le même esprit, lorsqu'on calcule modulo 9 la somme des chiffres d'un nombre, il peut être astucieux de grouper ceux dont la somme fait 9 ou un multiple de 9 : par exemple pour 12 791 : 1+1 = 2 $\equiv$ 2 [9].

Critère de divisibilité par 9

Le résultat précédent étant énoncé, le critère de divisibilité par 9 devient évident !

En effet, savoir si un nombre est divisible par 9 revient à savoir s'il est congru à 0 modulo 9... et donc, en appliquant le résultat précédent, cela revient à savoir si la somme de ses chiffres est congrue à 0 modulo 9.

Ainsi, on retrouve le critère de divisibilité par 9 :

« Un nombre entier est divisible par 9 si la somme de ses chiffres est elle-même divisible par 9. »

Fiche 1 Exercices	ARITHMÉTIQUE MODULAIRE (1)	Mathématiques pour l'informatique

Exercice 1 (méthode de la potence)

Effectuer la division euclidienne de a par b par la méthode de la potence dans les cas suivants :

- $a=73$ et $b=21$
- $a=1267$ et $b=5$
- $a=6359$ et $b=157$
- $a=32656$ et $b=157$

Exercice 2 (divisibilité par 25)

1) En écrivant 1 375 sous la forme 1 300 + 75, montrer que 1 375 est divisible par 25.
2) Le nombre 39 850 est-il divisible par 25 ? Et le nombre 28 235 ?
3) En déduire un critère simple de divisibilité par 25.

Exercice 3 (divisibilité par 16)

1) Vérifier que 10 000 est divisible par 16.
2) En écrivant 79 532 512 sous la forme 79 530 000 + 2 512, montrer que 79 532 512 est divisible par 16.
3) Le nombre 134 496 est-il divisible par 16 ? Et le nombre 131 964 ?
4) En déduire un critère simple de divisibilité par 16.

Exercice 4 (divisibilité par 2^p)

1) Exemple : vérifier (en divisant par 2 six fois de suite) que le nombre 164 928 est divisible par $2^6 = 64$. En déduire, sans calcul, que 543 737 164 928 est divisible par 64.
2) Soit p un entier naturel non nul.
   a) Expliquer pourquoi 10^q est divisible par 2^p, pour tout entier naturel $q \geqslant p$.
   b) En déduire qu'un entier est divisible par 2^p si le nombre formé par ses p derniers chiffres (chiffres de droite) est divisible par 2^p.

Exercice 5 (décomposition en produit de facteurs premiers)

Décomposer en produit de facteurs premiers les nombres :

- $a = 135\,828$
- $b = 36\,100$
- $c = 66\,654$
- $d = 797\,511$
- $e = 271\,825$
- $f = 163\,009$
- $g = 671\,099$
- $h = 214\,375$
- $i = 113\,989\,114$
- $j = 2\,416\,729$.

Exercice 6

En décomposant a et b en produits de facteurs premiers, déterminer $PGCD(a;b)$ et $PPCM(a;b)$ dans les cas suivants :

a	5383	420	978	272
b	4095	550	224	228

Exercice 7

Calculer, dans chacun des cas, en utilisant l'algorithme d'Euclide, le *PGCD* et le *PPCM* de a et b.

a	657 405	8 753	544	65	204	54 865
b	405	147	493	26	206	44 685

Exercice 8

Si $n \in \mathbb{N}$, expliquer pourquoi, à l'aide de Bachet-Bezout, le nombres n et $n+1$ sont premiers entre eux.

Exercice 9

Pour les entiers a et b ci-dessous, à l'aide de l'algorithme d'Euclide étendu, des entiers (relatifs) x et y tels que $ax+by=PGCD(a;b)$:

a	12	-11	150	138 807
b	42	25	54	52 089

Exercice 10

Déterminer les affirmations exactes dans la liste suivante :

$17\equiv 45[5]$ $17\equiv -18[5]$ $175\equiv 2[7]$ $15\equiv 3[7]$ $544\equiv 4[10]$ $151\equiv 1[2]$ $25\equiv 43[17]$
$100\equiv 1[11]$ $1000\equiv 10[11]$ $1000\equiv -1[11]$ $7852\equiv 1[4]$

Exercice 11 : congruence et PGCD

Soient a,b et c trois entiers naturels non nuls tels que $a\equiv b[c]$.

1) Soit d un diviseur commun de a et c. Montrer que d est un diviseur commun de b et c.
2) Soit d un diviseur commun de b et c. Montrer que d est un diviseur commun de a et c.
3) En déduire que $PGCD(a,c)=PGCD(b,c)$.
4) Trouver un exemple qui montre que la réciproque est fausse.

Exercice 12 : critères de divisibilité

Utiliser les règles de la congruence pour retrouver les critères de divisibilité par 2, 3, 5, 10 et 11.

$45-17=28$ pas un multiple de 5.

$17-(-18)=35$.
$-18-13=-35$

Fiche 3 Exercices	ARITHMÉTIQUE MODULAIRE (1)	Mathématiques pour l'informatique

Exercice 1 (tiré de Nouvelle Calédonie 2013)

Une équipe d'étudiants implante un virus sur un ordinateur.
Le nombre de fichiers infectés en fonction du nombre n d'allumages de l'ordinateur est 3^n-1.
Par ailleurs, chaque fois que le nombre de fichiers infectés est un multiple de 11, un message d'avertissement s'affiche à l'écran.
Le reste de la division euclidienne de 3^n-1 par 11 est noté W_n.

1) Recopier et compléter le tableau suivant :

n	3^n-1	W_n
1		
2		
3		
4		
5		

2) Démontrer que si n est un multiple de 5, alors $3^n-1\equiv 0$ (modulo 11).
Quelle information peut-on en déduire sur l'apparition du message d'avertissement ?

Exercice 2 (Métropole 2013)

Un jeu classique consiste à coder des messages. Pour cela, on utilise la correspondance entre les lettres de l'alphabet et un nombre entier x compris entre 0 et 25.
Le tableau ci-dessous donne cette correspondance :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le codage consiste à choisir une clé formée de deux nombres entiers a et b compris entre 0 et 25 et à remplacer une lettre par une autre selon le principe suivant :
- on lit sur le tableau le nombre x correspondant à la lettre ; on calcule le reste r de la division de $ax+b$ par 26 ;
- on lit sur le tableau la lettre correspondant au nombre r qui est donc la lettre codée.

Exemple : avec la clé $(a\,;\,b)=(7\,;\,12)$, pour coder la lettre T, on calcule $7\times 19+12=145$, puis le reste de la division euclidienne de 145 par 26, soit 15. La lettre codée est ainsi la lettre P.

1. Coder les lettres A, K et W avec la clé $(a\,;\,b)=(5\,;\,17)$.
2. Que se passe-t-il si on prend $a=0$ et $b=17$?
3. On considère un entier x compris entre 0 et 25.
   a. Donner, sans justification, les restes obtenus dans la division euclidienne de $13x+6$ par 26 pour x compris entre 0 et 25.
   b. Coder le mot PREMIER avec la clé (13 ; 6). Commenter le résultat obtenu.
4. Un codage est dit acceptable lorsque deux lettres distinctes quelconques sont toujours codées différemment. On admet que les clés $(a\,;\,b)$ donnant un codage acceptable sont celles pour lesquelles a est un entier premier avec 26, quel que soit l'entier b compris entre 0 et 25.
   a. Donner la liste des nombres entiers compris entre 0 et 25 et premiers avec 26.
   b. Déterminer le nombre de clés donnant un codage acceptable.
5. Le mot ABSURDE a été codé à l'aide d'une clé $(a\,;\,b)$ selon le principe décrit ci-dessus et l'on a obtenu VOZLGAT. Déterminer cette clé.

Exercice (Polynésie mai 2013)

Le but de cet exercice est l'étude d'un procédé de cryptage des lettres majuscules de l'alphabet français. Chacune des 26 lettres est associée à l'un des entiers de 0 à 25, selon le tableau de correspondance suivant.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le cryptage se fait à l'aide d'une clé, qui est un nombre entier k fixé, compris entre 0 et 25.

Pour crypter une lettre donnée :

- on repère le nombre x associé à la lettre, dans le tableau de correspondance précédent ;
- on multiplie ce nombre x par la clé k ;
- on détermine le reste r de la division euclidienne de $k \times x$ par 26 ;
- on repère la lettre associée au nombre r dans le tableau de correspondance ; c'est la lettre cryptée.

Par exemple, pour crypter la lettre « P » avec la clé $k = 11$:

- le nombre x associé à la lettre « P » est le nombre 15 ;
- on multiplie 15 par la clé k, ce qui donne $11 \times 15 = 165$;
- on détermine le reste de 165 dans la division par 26 : on trouve 9 ;
- on repère enfin la lettre associée à 9 dans le tableau : c'est « J ».

Ainsi, avec la clé $k = 11$, la lettre « P » est cryptée en la lettre « J ».

On crypte un mot en cryptant chacune des lettres de ce mot.

Partie A - Cryptage d'un mot avec la clé $k = 11$

Dans cette partie, la clé de cryptage est $k = 11$. Le but de cette partie est de crypter le mot « BTS ».

1. Déterminer en quelle lettre est cryptée la lettre « S ». On détaillera les différentes étapes du processus de cryptage.
2. Crypter le mot « BTS ». On ne demande pas le détail du cryptage.

Partie B - Décryptage avec la clé $k = 11$

Dans cette partie, la clé de cryptage est toujours $k = 11$.

Le but de cette partie est de retrouver une lettre initiale connaissant la lettre cryptée.

1. Prouver que $19 \times 11 \equiv 1 \mod 26$.
2. Une lettre associée à un nombre x a été cryptée. Le nombre associé à la lettre cryptée est noté y.
   a. Justifier que $11 \times x \equiv y \mod 26$.
   b. Montrer que $19 \times y \equiv x \mod 26$.

   Ces propriétés montrent que pour décrypter une lettre codée y avec la clé $k = 11$, il suffit de crypter cette lettre avec la clé de cryptage $k' = 19$.

   Exemple : si une lettre est codée par $y = 22$, on multiplie 22 par 19 et on prend le reste du résultat dans la division euclidienne par 26 ; on obtient $x = 2$. Donc la lettre de départ est C.
3. Utiliser les résultats précédents pour décrypter le mot « WGA ».

Partie C - Recherche des bonnes clés de cryptage

Une clé k ne possède pas forcément une clé de décryptage associée.

On dit qu'une clé est une bonne clé de cryptage si elle possède une clé de décryptage associée.

On admet qu'une clé k est une bonne clé de cryptage si et seulement si les nombres k et 26 sont premiers entre eux.

Le but de cette partie est de trouver les bonnes clés de cryptage, parmi les nombres entiers compris entre 0 et 25.

1. Décomposer 26 en un produit de facteurs premiers.
2. En déduire la liste des nombres k compris entre 0 et 25 qui sont de bonnes clés de cryptage.