SIO1	Arithmétique : étude des nombre entiers	feuille **1**

I. Multiples et diviseurs

Définition: si a, b, c sont trois nombres entiers tels que $a=b\times c$
alors
on dit que a est un . . . . de b et de c
et
on dit que b et c sont des . . . . de a

Exemples :
> Liste des diviseurs de 12 :

> Liste des multiples de 12 :

Remarque : chaque entier non nul a une infinité de . . . .

et un nombre fini de . . . .

>Liste des multiples de 7 compris entre 75 et 100 :

Exercice 1
1) Donner la liste des multiples de 13 compris entre 700 et 800

2) 65 est-il multiple de 13 ? Justifier !

3) Donner la liste des diviseurs de 13 :

Définition : un nombre *premier* est un entier qui a exactement deux diviseurs.
Par exemple : 2,3, 5, 7, 11... sont des nombres premiers

Vocabulaire : un nombre **composé** est un entier qui n'est pas premier.
On peut donc le « décomposer » en produit de deux entiers inférieurs.

Ex : $15=...\times...$

Liste des nombres premiers inférieurs à 100
On utilise la méthode du « crible d'Eratostène » :
Parmi tous les entiers de 2 à 100, on élimine tous ceux qui sont composés : il ne reste donc que les nombres premiers.

	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

Exercice 2
1) Décomposer au maximum les nombres entiers suivants :

$7000=...\times...$

$297=...\times...$

2) En déduire la liste de TOUS les diviseurs de 297

3) Déterminer la liste de tous les diviseurs de 7000

SIO1	**Arithmétique : étude des nombre entiers**	feuille **2**

Méthode pour tester si un nombre est premier

<u>Exemple</u> : Tester si le nombre 397 est premier
> on teste si 397 admet un diviseur autre que 1 et 397

Puisque $\sqrt{397} \approx 19{,}9$ il suffit de tester les diviseurs inférieurs à . . .

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Plus généralement, pour tester si un entier N est premier :

- calculer $\sqrt{N}$
- pour chaque nombre premier p entre 2 et $\sqrt{N}$: diviser N par p
  - si le résultat est entier → N est composé : il est multiple de p !
- si N n'est multiple d'aucun des entiers p , alors il est premier.

Exercice 3: les entiers suivants sont premiers ?
- si oui : justifier
- sinon : les décomposer « au maximum »

a = 999 b = 733 c = 1492

Propriété : tout nombre entier $n \geq 2$ s'écrit comme produit de nombres premiers $\boxed{n = p_1^{n_1} \times p_2^{n_2} \times \ldots \times p_k^{n_k}}$
avec p_1 , p_2 , … , p_k premiers et n_1 , n_2 , …, n_k entiers

Exercice 4
1) Décomposer en produit de facteurs premiers le nombre N = 350
2) En déduire la liste des diviseurs de 350.

Exercice 5
1) Donner la liste des diviseurs de 60
2) Donner la liste des diviseurs de 150
3) Déterminer le plus grand diviseur commun de 60 et 150

SIO1 **Arithmétique : étude des nombre entiers** feuille **3**

II. Plus grand diviseur commun

1. Définition

On note PGCD(a ; b) le Plus Grand Commun Diviseur de deux entiers a et b .

Exemple :
Les diviseurs de 60 sont : 1 2 3 4 5 6 10 12 15 20 30 60
Les diviseurs de 150 sont : 1 2 3 5 6 10 15 25 30 50 75 150
Les diviseurs communs à 60 et 150 sont donc : 1 2 3 5 6 … … …
donc : PGCD(60;150) = …

2. Recherche du pgcd avec les diviseurs premiers

si on connaît la décomposition en produit de facteurs premiers de deux entiers a et b , il est facile de trouver celle de leur pgcd.

Exemple : $a=294\,000=2^4\times3^1\times5^3\times7^2$
et $b=118300=2^2\times5^5\times7^1\times13^2$

Un diviseur d commun à a et b aura une décomposition de la forme $d=2^{n_1}\times5^{n_2}\times7^{n_3}$

→ calcul de n_1 : pour que 2^{n_1} divise a **et** b , on doit avoir :
n_1 = … ou n_1 = … ou n_1 = …
Pour que d soit le plus grand possible, il faut que $n_1=$... .

→ pour chaque diviseur premier commun à a et b , on conserve **le plus petit des deux exposants** correspondant à ce nombre premier dans la décomposition de a et dans celle de b .

On a donc dans cet exemple :
$d=pgcd\left(2^4\times3^1\times5^3\times7^2 ; 2^2\times5^5\times7^1\times13^2\right)=2^{\cdots}\times3^{\cdots}\times5^{\cdots}\times7^{\cdots}\times13^{\cdots}=3500$

Exercice 6

1) Décomposer chaque entier en produit de facteurs premiers
$a=13000$ $b=2100$ $c=2015$ $d=2016$

2) En déduire :

a) PGCD(13000 ; 2015)

b) PGCD(2100 ; 2016)

3. Division euclidienne

Propriété et définition :
soit a et b deux entiers naturels.
Il existe un unique entier q et un unique entier r tels que :
$a=b\times q+r$ et $0\leq r<b$
On dit alors que : q est le . . . . et r le . . . . de la **division euclidienne** de a par b

Remarque 1 : à la calculatrice, 99/5=19,8
donc le quotient entier de 99 par 5 est . . . .
Pour calculer le reste, il suffit d'effectuer
$99-5\times19=4$ ou $0{,}8\times5=4$

Remarque 2 : en python, on peut calculer
le quotient entier de 99 par 5 :
le reste de 99 dans la division par 5 :

Exercice 7

Dans chaque cas, poser la division euclidienne de a par b , puis l'écrire « en ligne » sous forme $a=b\times q+r$.

1) $a=2000$ et $b=3$

2) $a=2000$ et $b=5$

3) $a=78$ et $b=83$

4. Calcul du pgcd de deux entiers : algorithme d'Euclide

Cet algorithme repose sur le fait qu'un diviseur d commun à a et b divise aussi le reste r de la division euclidienne de a par b.
On a donc : PGCD(a ; b) = PGCD(b ; r)
On itère le procédé jusqu'à ce que le reste r soit nul.
Le dernier reste non nul est le pgcd de a et b.

Exemple : cherchons pgcd (492 ; 42)
On calcule les restes successifs des divisions euclidiennes :

a	b	r
492	42	

Le dernier reste non nul est le pgcd de a et b donc **pgcd(492 ; 42)=. . .**

Exercice 8
Calculer les pgcd suivants avec l'algorithme d'euclide :

a) pgcd(1234 ; 21)

b) pgcd(156 ; 516)

c) pgcd(1365 ; 858)

Exercice 9 : algorithmique.
Écrire un algorithme qui lit deux entiers a et b, puis calcule leur pgcd avec l'algorithme d'Euclide.
Coder cet algorithme en python.

Algorithme

```
Variables
        a, b, r de type entier
début




fin
```

programme en python

```
# pgcd avec l'algorithme d'Euclide

a = . . .
b = . . .

while . . .
```

un premier exemple de fonction en python

```
def pgcd(a, b) :
```

SIO1	Arithmétique : étude des nombre entiers	feuille **4**

III. <u>Nombre premiers entre eux</u>

Définition : deux entiers naturels a et b sont ***premiers entre eux*** si $PGCD(a,b)=1$.
Cela signifie que deux nombre premiers entre eux n'ont aucun diviseur commun (sauf …)

Exemple :
pgcd(1234 ; 21)=1 donc …

pgcd(516 ; 156) = 12 donc …

<u>Remarque</u> : ne pas confondre « premier » (au singulier) avec « premiers entre eux » ou « premier avec... » (au pluriel)

Exercice 10 VRAI ou FAUX ?

a) 7 est premier

b) 21 est premier

c) 21 et 25 sont premiers entre eux

d) 21 et 25 sont premiers

e) 7 est premier avec 21

Exercice 11
Les entiers suivants sont-ils premiers entre eux ?

a) 123456 et 122

b) 111 et 370

c) 17 et 2000

IV. Congruences

Quelques calculs pour commencer

0	1	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

Si on poursuit le tableau , dans quelle colonne seront rangés les nombres suivants ?

$A=85+67$

$B=79\times 73$

$C=15^8$

$D=2^{10}$

SIO1	Arithmétique : étude des nombre entiers	feuille 5

IV. Congruences

1. Définition

Déf : Soit n un entier naturel non nul. On dit que deux entiers a et b sont **congrus modulo n** et on note $\boxed{a \equiv b[n]}$ si a et b ont même reste dans la division euclidienne par n.

Exemple 1 : congruences modulo 7

$$\begin{array}{r|l} 15 & 7 \\ \hline & 2 \end{array} \quad \text{et} \quad \begin{array}{r|l} 365 & 7 \\ \hline & 52 \end{array}$$

15 et 365 ont même reste : 1, dans la division euclidienne par 7
donc $365 \equiv 15[7]$

Remarque : travailler avec des congruences modulo 7 revient à ranger tous les entiers en 7 colonnes (numérotées de … à …)
Deux nombres sont congrus modulo 7 s'ils sont situés dans la même colonne !

Exemple 2 : $\begin{array}{r|l} 63 & 7 \\ \hline 0 & 9 \end{array}$ donc $63 = 7 \times ... + ...$ et donc $63 \equiv ...[...]$
autrement dit « 63 est multiple de 7 »

A retenir:

➔ si $a = \boldsymbol{n} \times k + r$ (avec k et r entiers) alors : $a \equiv r[\boldsymbol{n}]$

➔ $a \equiv 0[n]$ signifie que …

2. Propriétés

Les congruences modulo n sont compatibles avec l'addition et la multiplication.
Théorème (admis) les congruences sont compatibles avec l'addition et la multiplication.
Si a, a', b, b' sont des entiers tels que $a \equiv a'[n]$ et $b \equiv b'[n]$ alors

$$a + b \equiv a' + b'[n]$$

$$a \times b \equiv a' \times b'[n]$$

$$a^k \equiv a'^k[n].$$

Exemple 3 : $365 \equiv 1[7]$ donc $366 \equiv ...[7]$
application : quel jour de la semaine serons-nous dans 4 ans ?
Nombre de jours dans une durée de 4 ans :

Exemple 4 : $10 = 7 \times 1 + 3$ donc $\boxed{10 \equiv 3[7]}$

en élevant au carré : $10^2 \equiv .....[7]$ donc $100 \equiv ...[7]$

et puisque $9 \equiv ...[7]$ on a donc aussi $\boxed{100 \equiv ...[7]}$

$1000 = 10 \times 100 \equiv ... \times ...[7]$ donc $\boxed{1000 \equiv 6[7]}$

Application : réduire 1789 modulo 7
$1789 = 1 \times 1000 + 7 \times 100 + 8 \times 10 + 9$ donc

$1789 \equiv 1 \times .... + ... \times ..... + ... \times ... + ...[7]$

$1789 \equiv ......[7]$ ce qui signifie que 1789 et …… ont le même reste dans la division euclidienne par 7 : ce reste vaut …

3. Utilisation : critère de divisibilité par 9

Soit N un nombre de quatre chiffres en base 10 : $N = abcd_{(10)}$

$N = a \times .... + b \times .... + c \times ... + d = ... \times 10^{...} + ... \times 10^{...} + ... \times 10^{...} + ...$

Réduire modulo 9 : $10 \equiv ...[9]$

$10^2 \equiv ... ...[9]$

$10^3 \equiv ... ...[9]$

donc $N \equiv ... ...[9]$

Conclusion : N et .... ont le même reste dans la division euclidienne par 9.
Pour tester si N est multiple de 9, il suffit donc d'ajouter tous ses chiffres, et de tester si la somme est multiple de 9.

Remarque : le même principe fonctionne aussi pour les multiples de 3.

Exercice 12
Si, aujourd'hui, nous sommes vendredi, quel jour de la semaine serons-nous dans 100 jours ? Et dans 1000 jours ?

Exercice 13 Vrai ou Faux ? Justifier.

a) $57\equiv 30[8]$ b) $111\equiv 36[5]$

c) $2014\equiv 75[7]$ d) $2014\equiv 5[7]$

Exercice 14
Compléter avec un entier convenable les congruences suivantes :

8≡…[10] 122≡ …[10] 453≡ … [10] 1400≡ …[10]

17≡…[7] 28≡ … [7] 155≡ … [7] 852≡ … [7]

Exercice 15
1) Trouver quatre entiers **différents** pour compléter

87 ≡ … [5] 87 ≡ … [5]

87 ≡ … [5] 87 ≡ … [5]

2) Comment peut-on décrire tous les entiers b tels que $87\equiv b[5]$?

Exercice 16

1) Établir que pour tout $n\in\mathbb{N}$, on a $10^n\equiv 1[3]$

2) Soit $N=4\times 10^4+7\times 10^3+2\times 10^2+1\times 10^1+5\times 10^0$
   a) Donner l'écriture décimale de N
   b) Quel est le reste de la division euclidienne de N par 3 ?

Exercice 17
Donner les restes de la division euclidienne des nombres suivants par 7 :

$a=50$ $b=50^{100}$ $c=100$

$d=100^2$ $e=50^{100}+100+100^2$

Exercice 18
quel est le reste de la division par 17 des nombres suivants : (justifier !)

200 200^2 200^3 200^4

Suivant les valeurs de $n\in\mathbb{N}$, quel est le reste de la division de 200^n par 17 ?

En déduire le reste la division de 200^{2013} par 17.

Exercice 19
Sachant que $n\equiv 3[5]$, montrer que $2n^2-n$ est un multiple de 5.

Exercice **20 : Application aux billets de banque**
Sur les billets de banque en euros figure un nombre de 11 chiffres décimaux précédé d'une lettre. En remplaçant cette lettre par son rang dans l'alphabet (de 1 à 26), on obtient ainsi un nombre de 12 ou 13 chiffres.
Le billet ne peut être authentique que si le reste de ce nombre dans la division par 9 vaut 8.

1. Les billets portant les numéros U57794585675 et S00212913867 peuvent-ils être authentiques ?
2. Un billet authentique porte le numéro T2303557409x (il y a une tache sur le dernier chiffre). Que vaut x ?
3. Le nombre figurant sur un billet authentique est 16122340243 mais la lettre est effacée. Quelle peut-être cette lettre ?