Chapitre 2

Arithmétique

Dans ce chapitre, sauf précision contraire, lorsqu'on parlera d'un *nombre*, il s'agira d'un nombre entier naturel.

2.1 Vocabulaire. Critères de divisibilité

2.1.1 Vocabulaire

Soit n, d, m trois entiers naturels avec $d \neq 0$.
- On dit que d est un diviseur de n si $\frac{n}{d}$ est un entier naturel. Dans ce cas on dit aussi que d divise n.
- On dit que m est un multiple de n s'il existe $k \in \mathbf{N}$ tel que $m = kn$.

Remarque 2.1
Si m est un multiple de n (où $n \neq 0$) alors n est un diviseur de m.

Exemple 2.1
- Les diviseurs de 60 sont : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.
- Les diviseurs de 100 sont : 1, 2, 4, 5, 10, 20, 25, 50, 100.
- Les multiples de 3 sont : 0, 3, 6, 9, 12, ...

```
1 Entrées :
2 Saisir N;
3 1 → D;
4 début
5     tant que D ≤ N faire
6         si N/D est entier alors
7             Afficher D
8         D + 1 → D;
9 fin
```

Algorithme 3 : recherche des diviseurs

Programme en langage Casio :
```
?→N
1→D
While D≤N
If N÷D=Int(N÷D)
Then D◢
IfEnd
D+1→D
WhileEnd
''FIN''
```

Programme en langage TI :
```
Input N
1→D
While D≤N
If N÷D=Int(N÷D)
Then
Disp D
Pause
End
D+1→D
End
```

2.1.2 Propriété

Propriété 2.1
Soit a, b et c trois entiers naturels non nuls.
- Si a divise b et si b divise c, alors a divise c.
- Si a divise b et si a divise c, alors a divise $b + c$, $b - c$, et même toute combinaison $\alpha b + \beta c$ où α et β sont des entiers relatifs quelconques.
- Si a divise b alors a divise αb pour tout $\alpha \in \mathbf{N}$.
- Si a divise b alors ac divise bc.

Exemple 2.2
Quelques illustrations numériques simples :
- on a : 3 divise 15 et 15 divise 75, donc 3 divise 75 ;
- on a : 7 divise 105 et 7 divise 42, donc 7 divise 105+42=147, 7 divise 105-42=63, et même 7 divise $5 \times 105 - 3 \times 42 = 399$;
- 9 divise 27 donc 9 divise $45 \times 27 = 1215$;
- 5 divise 35 donc $5 \times 3 = 15$ divise $35 \times 3 = 105$.

Démonstration de la propriété 2.1 :
- Si a divise b alors il existe $k \in \mathbf{N}$ tel que $b = ka$.
  Si b divise c alors il existe $k' \in \mathbf{N}$ tel que $c = k'b$.
  Donc : $c = k'b = k'ka$. Donc a divise c.
- Si a divise b alors il existe $k \in \mathbf{N}$ tel que $b = ka$.
  Si a divise c alors il existe $k' \in \mathbf{N}$ tel que $c = k'a$. Donc :
  $b + c = ka + k'a = a(k + k')$: c'est à dire que a divise $b + c$;
  $b - c = ka - k'a = a(k - k')$: c'est à dire que a divise $b - c$;
  $\alpha b + \beta c = \alpha ka + \beta k'a = a(\alpha k + \beta k')$: c'est à dire que a divise $\alpha b + \beta c$.
- Si a divise b alors il existe $k \in \mathbf{N}$ tel que $b = ka$.
  Donc $\alpha b = \alpha ka$ et ainsi a divise αb.
- Si a divise b alors il existe $k \in \mathbf{N}$ tel que $b = ka$.
  Donc $bc = kac$ et ainsi ac divise bc.

Exemple 2.3
Déterminer les entiers naturels n tels que $n + 1$ divise $2n + 5$.
$n + 1$ divise $n + 1$ et il divise $2n + 5$.
Donc d'après la propriété 2.1, $n + 1$ divise $(2n + 5) - 2 \times (n + 1) = 2n + 5 - 2n - 2 = 3$.

C'est à dire que $n+1$ divise 3. Donc $n+1$ peut être égal à 1 ou à 3. Ainsi les valeurs possibles de n sont 0 ou 2.
Vérifions : si $n=0$ on a bien 1 qui divise 5 ; et si $n=2$ on a bien 3 qui divise 9. Les valeurs de n possibles sont donc 0 et 2.

2.1.3 Critères de divisibilité

Propriété 2.2 (Critères de divisibilité)
- Un nombre est divisible par 2 si et seulement si son chiffre des unités est un 0, un 2, un 4, un 6 ou un 8.
- Un nombre est divisible par 5 si et seulement si son chiffre des unités est un 0 ou un 5.
- Un nombre est divisible par 4 (resp. 25) si et seulement si le nombre formé par les deux derniers chiffres (dizaines et unités) est un multiple de 4 (resp. 25).
- Un nombre est divisible par 3 (resp. 9) si et seulement si la somme de ses chiffres est un multiple de 3 (resp. 9).
- Un nombre est divisible par 11 si et seulement si la différence entre la somme des chiffres de rang impair et la somme des chiffres de rang pair est un multiple de 11.

Démonstration :
Soit $N=\ldots edcba$ un entier.
- On a : $N=a+10b+100c+\cdots=a+2(5b+50c+\ldots)$. Ainsi en utilisant la propriété 2.1, on a N divisible par 2, $2(5b+50c\ldots)$ divisible par 2, donc a est divisible par 2. Ainsi si N est divisible par 2 alors son chiffre des unités est pair. La réciproque est claire.
- On a $N=a+5(2b+20c+\ldots)$. On utilise alors une démonstration analogue à la précédente.
- On a $N=(a+10b)+4(25c+250d+\ldots)=(a+10b)+25(4c+40d+\ldots)$. On utilise alors une démonstration analogue à la première.
- $N=a+(9+1)b+(99+1)c+\cdots=(a+b+c+\ldots)+3\times3(b+11c+111d+\ldots)$. On utilise alors une démonstration analogue à la première.
- $N=(a+100c+\ldots)+(10b+1\,000d+\ldots)=(a+c+99c+\ldots)+(11b-b+1\,001d-d+\ldots)=(a+c+\ldots)-(b+d+\ldots)+11(9c+\cdots+b+91d+\ldots)$. On utilise alors une démonstration analogue à la première.

Exemple 2.4
Soit $N=6\,285$. N est divisible par 5 mais pas par 2.
Il est divisible par 3, mais pas par 9 $(6+2+8+5=21=3\times7)$.
Il n'est pas divisible par 11 $((6+8)-(2+5)=7)$.
Soit $M=7\,392$. M est divisible par 2 mais pas par 5.
Il est divisible par 3 mais pas par 9.
Il est divisible par 11 $((7+9)-(3+2)=11)$.

2.2 Les nombres premiers

Définition 2.1
Un nombre premier est un entier strictement supérieur à 1 qui n'est divisible que par 1 et par lui-même.

Exemple 2.5
2 est un nombre premier, 11 aussi.

10 n'est pas un nombre premier car il est divisible par 5.

Propriété 2.3
Pour savoir si un nombre n est premier, on teste sa divisibilité par tous les nombres premiers inférieurs ou égaux à $\sqrt{n}$.
Si aucun de ces nombres ne divise n, alors n est un nombre premier, sinon, il ne l'est pas.

Crible d'Ératosthène (3^{e} siècle av. J.-C.)
On regroupe dans un tableau tous les entiers inférieurs à 100 (par exemple), on barre 1, puis on entoure 2. On barre alors tous les multiples de 2. Le premier entier suivant non barré est premier : il s'agit de 3. On barre tous les multiples de 3 ; le premier entier suivant 3 non barré est premier : c'est 5 etc.…

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
91	92	93	94	95	96	97	98	99	100

Ici, les nombres non premiers sont écrits en rouge. Les nombres premiers inférieurs à 100 sont donc :
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.

Théorème 2.1
- Tout entier strictement supérieur à 1 admet un diviseur premier.
- Il existe une infinité de nombres premiers.

Démonstration :
- Soit n un entier strictement supérieur à 1. Si n est premier, il est divisible par lui-même donc par un nombre premier.
  Si n n'est pas premier, il s'écrit $n=d\times m$ avec $1<d<n$. Si d est premier, la démonstration est terminée, et si d n'est pas premier on a $d=d'\times m'$ avec $1<d'<d$. d' est alors un diviseur de d et de n (cf. prop 2.1). Et on recommence l'étape précédente. Comme $n>d>d'>\ldots$, il existe un « $d^{(p)}$ » qui est premier.
- Raisonnons par l'absurde : on suppose qu'il y a un nombre fini de nombres premiers. On les note p_1, p_2,…, p_n.
  Soit $N=p_1\times p_2\times\cdots\times p_n+1$. Ce nombre admet un diviseur premier p qui est un des p_i où $1\leq i\leq n$.
  Ainsi, p divise N et p divise $p_1\times p_2\times\cdots\times p_n$, donc il divise la différence de deux (propriété 2.1). Donc p divise 1 et donc $p=1$. C'est absurde car p est un nombre premier il est donc strictement plus grand que 1.
  On aboutit à une absurdité, notre supposition de départ est donc fausse. On a ainsi démontré qu'il y a une infinité de nombres premiers.

Exemple 2.6
Le nombre $P = n^2 + 2n + 1$ où $n \in \mathbf{N}$ peut-il être premier ?
On a $n^2 + 2n + 1 = (n + 1)^2$. Si $n = 0$ alors $P = 1$: il n'est pas premier.
Si $n > 0$, P est divisible par $n + 1$ qui est différent de 1 et de P donc il n'est pas premier.

2.3 Décomposition en produit de facteurs premiers

2.3.1 Théorème de décomposition

Théorème 2.2
Tout entier strictement supérieur à 1 se décompose en un produit de facteurs premiers. Cette décomposition est unique, à l'ordre près des facteurs.

Démonstration : (existence)
Soit N un entier strictement supérieur à 1.
Si N est premier, la décomposition est « $N = N$ ».
Si N n'est pas premier, il admet (au moins) un diviseur premier (théorème 2.1). Soit p_1 le plus petit d'entre eux. On a : $N = p_1 \times q_1$, avec $q_1 < N$.
Si q_1 est premier la démonstration est terminée, sinon, on recommence le même procédé avec q_1 : $q_1 = p_2 \times q_2$ avec p_2 premier et $q_2 < q_1$, ... Il finit par y avoir un $q_n = 1$ car les q_n sont de plus en plus petits.
Finalement on obtient $N = p_1 \times p_2 \times \cdots \times p_n \times 1 = p_1 \times p_2 \times \cdots \times p_n$

Remarque 2.2
Dans la décomposition en produit de facteurs premiers, un même facteur peut apparaître plusieurs fois. On écrit alors :

$$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}, \text{ avec } p_i \text{ premiers et } 1 \leq \alpha_i$$

Exemple 2.7
$60 = 2^2 \times 3 \times 5$;
$100 = 2^2 \times 5^2$;
$2\,100 = 2^2 \times 3 \times 5^2 \times 7$

```
1  Entrées :
2  Saisir N;
3  2 → P;
4  début
5      tant que P ≤ N faire
6          si N/P est entier alors
7              Afficher P;
8              N/P → N;
9          sinon
10             P + 1 → P
11 fin
```

Algorithme 4 : décomposition en produit de facteurs premiers

Programme en langage Casio :

```
?→N:2→P
While P≤N
If N÷P=Int(N÷P)
Then N÷P→N
P◢
Else P+1→P
IfEnd
WhileEnd
"FIN
```

Programme en langage TI :

```
Input N
2→P
While P≤N
If N÷P=Int(N÷P)
Then
N÷P→N
Disp P
Pause
Else
P+1→P
End
End
```

2.3.2 Application : détermination des diviseurs d'un entier

Exemple 2.8
La décomposition en produit de facteurs premiers de 20 est : $20 = 2^2 \times 5$. Pour trouver tous les diviseurs de 20 (et non pas seulement les diviseurs premiers), on effectue tous les produits possibles avec les facteurs de la décomposition ci-dessus (et on a aussi 1 comme diviseur).
On a donc comme diviseurs de 20 :
$d_1 = 1$, $d_2 = 2$, $d_3 = 2^2 = 4$, $d_4 = 5$, $d_5 = 2 \times 5 = 10$, $d_6 = 2^2 \times 5 = 20$.

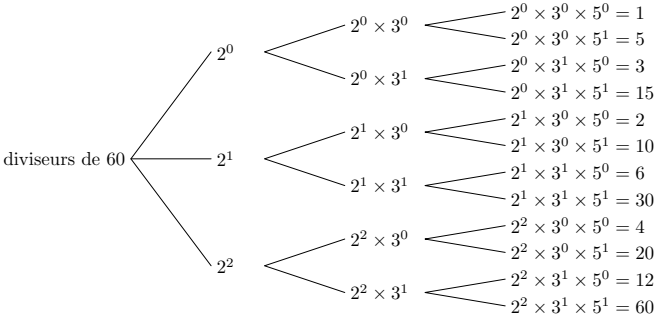
Généralisation :
Si N est un entier dont la décomposition en produit de facteurs premiers est :

$$N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}, \text{ avec } p_i \text{ premiers et } 1 \leq \alpha_i$$

Alors, les diviseurs de N sont les nombres qui s'écrivent :

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_n^{\beta_n}, \text{ avec : } 0 \leq \beta_i \leq \alpha_i$$

Exemple 2.9
En utilisant la décomposition en produit de facteurs premiers de 60, déterminer tous ses diviseurs.



Même question[1] pour 1 078

[1] Laissée en exercice au lecteur consciencieux

Remarque 2.3
Avec les notations de la généralisation précédente, le nombre de diviseur de N est :

$$(\alpha_1 + 1) \times (\alpha_2 + 1) \times \cdots \times (\alpha_n + 1)$$

2.4 Pgcd de deux entiers

2.4.1 Définition

Exemple 2.10
Les diviseurs de 24 sont : 1, 2, 3, 4, 6, 8, 12 et 24.
Les diviseurs de 36 sont : 1, 2, 3, 4, 6, 9, 12, 18 et 36.
24 et 36 ont 6 diviseurs en commun. Le plus grand d'entre eux est 12.

Propriété 2.4
Soit a et b deux entiers naturels non nuls. Il existe toujours au moins un diviseur commun à a et b. Le plus grand d'entre eux est appelé *Plus Grand Commun Diviseur*.
On le note pgcd(a, b).

Exemple 2.11
En écrivant la liste de leurs diviseurs, déterminer le pgcd des entiers 60 et 100.

2.4.2 Recherche du pgcd : algorithme d'Euclide

Propriété 2.5
Soit a et b deux entiers naturels tels que $a > b > 0$. On note respectivement q et r le quotient et le reste de la division euclidienne[2] de a par b.
On a alors : pgcd(a,b)=pgcd(b,r).

Démonstration :
Soit d =pgcd(a, b) et d' =pgcd(b, r).
On a d divise a et d divise b donc d divise $a - bq$ (propriété 2.1). C'est à dire que d divise r. Ainsi d est un diviseur de b et de r. Donc $d \leq$pgcd(b,$r = d'$).
De plus, d' divise b et d' divise r ; donc d' divise $bq + r$ (propriété 2.1). C'est à dire que d' divise a (et il divise b aussi). Or le plus grand diviseur commun à b et a est d. Donc $d' \leq d$.
Finalement, puisque $d \leq d'$ et $d' \leq d$, on peut conclure que $d' = d$ et ainsi pgcd(a,b)=pgcd(b,r).

Exemple 2.12
On prend $a = 102$ et $b = 30$. En écrivant les diviseurs de 102 et 30 on aboutit facilement à pgcd(102,30)=6.
La division euclidienne de 102 par 30 donne $q = 3$ et $r = 12$. Et pgcd(30,12)=6.

Algorithme d'Euclide :
Si on se donne deux nombres entiers non nuls et qu'on souhaite calculer leur pgcd, la propriété 2.5 permet de se ramener à un calcul de pgcd de deux nombres plus petits que les nombres de départ. En l'appliquant plusieurs fois successivement on obtient des restes de plus en plus petits, et ces derniers étant entiers, il finissent par atteindre 0. Le dernier reste non-nul est alors le pgcd des deux nombres de départ. Ce procédé est appelé *algorithme d'Euclide*.

[2] On a alors $a = bq + r$ avec $0 \leq r < b$


```
1 Entrées :
2 a et b deux entiers tels que a > b;
3 début
4     tant que b ≠ 0 faire
5         La division euclidienne de a par b donne un quotient q et un reste r;
6         b → a;
7         r → b;
8     Afficher : le pgcd est a;
9 fin
```

Algorithme 5 : algorithme d'Euclide

2.4.3 Calculatrices

Casio :

```
?→A
?→B
While B>0
Int(A÷B)→Q
A-B*Q→R
Q◢
R◢
''.....''
B→A
R→B
WhileEnd
"Le PGCD est :"◢
A◢
```

TI :

```
Prompt A
Prompt B
While B>0
Int(A÷B)→Q
A-B*Q→R
Disp Q
Disp R
''.....''
Pause
B→A
R→B
End
Disp"Le PGCD est :"
Disp A
```

2.4.4 Application

Théorème 2.3
L'ensemble des diviseurs communs à deux entiers non nuls est l'ensemble des diviseurs de leur pgcd.

Démonstration :
Soit a et b deux entiers non nuls et d leur pgcd. On a : $a = da'$ et $b = db'$.
- Soit n un diviseur de d alors n divise $a'd = a$ et n divise $b'd = b$ (propriété 2.1).
- Réciproquement, soit n un diviseur de a et de b. Montrons que n divise d : on a vu dans la démonstration de la propriété 2.5 que si n divise a et b alors il divise aussi r ; où r est le reste de la division euclidienne de a par b (si $a \geq b$). En réitérant le procédé plusieurs fois, on aboutit à : « n divise le dernier reste non nul de l'algorithme d'Euclide ». Or ce dernier reste non nul est le pgcd de a et b. On a donc montré que si n est un diviseur commun à a et b alors il est un diviseur de leur pgcd.

Finalement, l'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de leur pgcd.

Exemple 2.13
En utilisant le calcul du pgcd par l'algorithme d'Euclide, déterminer les diviseurs communs à 107 448 et 51 282.

2.4.5 Nombres premiers entre eux

Définition 2.2
Deux nombres sont dits *premiers entre eux* s'ils n'ont pas d'autre diviseur commun que 1.

Remarque 2.4
La définition revient à dire que deux nombres sont premiers entre eux si leur pgcd vaut 1.

Exemple 2.14
26 et 15 sont premiers entre eux.
32 et 30 ne sont pas premiers entre eux : ils sont tous les deux divisibles par 2.
1 088 et 3 213 sont-ils premiers entre eux ?

2.5 Complément

Un programme de recherche des diviseurs « optimisé » pour limiter le temps de recherche de la calculatrice :

Programme en langage Casio :

```
?→N
1→D
While D≤ √N
If N÷D=Int(N÷D)
Then D◢
N/D◢
IfEnd
D+1→D
WhileEnd
''FIN''
```

Programme en langage TI :

```
Input N
1→D
While D≤ √N
If N÷D=Int(N÷D)
Then
Disp D
Disp N/D
Pause
End
D+1→D
End
```