

## IV) NOTIONS D'ARITHMÉTIQUE.

## 1) Division euclidienne.

## a) Théorème de la division euclidienne :

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{N}^* \quad \exists! (q, r) \in \mathbb{Z}^2 / \boxed{a = bq + r} \text{ avec } 0 \leq r < b.$$

$q$  est le *quotient* de la division euclidienne de  $a$  par  $b$ , noté  $\text{quotient}(a, b)$  (pour Maple :  $\text{iquo}(a, b)$  : (integer quotient) ; pour Mathematica :  $\text{Quotient}[a, b]$ ).

$r$  est le *reste* de la division euclidienne de  $a$  par  $b$ , noté  $\text{reste}(a, b)$  (pour Maple :  $a \bmod b$  ou  $\text{irem}(a, b)$  : (integer remainder) ; pour Mathematica :  $\text{Mod}[a, b]$ )

D1

$$\text{REM : en fait } q = \left\lfloor \frac{a}{b} \right\rfloor = E\left(\frac{a}{b}\right) \text{ et } r = b \left\{ \frac{a}{b} \right\} = b \cdot \text{FRAC}\left(\frac{a}{b}\right).$$

b) Application à la forme générale des sous-groupes de  $\mathbb{Z}$ .

TH : les sous-groupes additif de  $\mathbb{Z}$  sont les parties de la forme  $a\mathbb{Z}$ .

D2

## 2) Systèmes de numération.

## a) Définitions.

Théorème de la décomposition d'un entier naturel en base  $b$  (dite *binaire* si  $b = 2$ , *décimale* si  $b = 10$ , *hexadécimale* si  $b = 16$ ):

$$\forall (a, b) \in \mathbb{N}^* \times \mathbb{N}^* \setminus \{1\} \quad \exists! n \in \mathbb{N} \quad \exists! (r_0, r_1, \dots, r_n) \in \prod_{k=0}^n [0, b-1]$$

$$\boxed{a = r_0 + r_1 b + r_2 b^2 + \dots + r_n b^n = \sum_{k=0}^n r_k b^k} \text{ avec } r_n \neq 0$$

$$\text{Notation : } a = \sum_{k=0}^n r_k b^k = \overline{r_n r_{n-1} \dots r_1 r_0}^{\text{base } b}; \text{ les } r_k \text{ sont les "chiffres" de } a \text{ en base } b.$$

D3

REM 1 : ce théorème n'est autre que le théorème de la division euclidienne itéré ; en effet la décomposition de  $a$  en base  $b$  s'obtient par l'algorithme :

$\begin{cases} r_0 = \text{reste}(a, b) \\ q_1 = \text{quotient}(a, b) \end{cases}$
$\begin{cases} r_1 = \text{reste}(q_1, b) \\ q_2 = \text{quotient}(q_1, b) \end{cases}$
$\dots$
$\begin{cases} r_k = \text{reste}(q_k, b) \\ q_{k+1} = \text{quotient}(q_k, b) \end{cases}$
$\dots$
$\begin{cases} r_n = \text{reste}(q_n, b) \\ q_{n+1} = \text{quotient}(q_n, b) = 0 \end{cases}$

REM 2 : en base 2, cet algorithme s'écrit plus simplement sous la forme :

$\begin{cases} r_0 = 0 \text{ si } a \text{ est pair, } 1 \text{ s'il est impair} \\ q_1 = \left\lfloor \frac{a}{2} \right\rfloor \end{cases}$
$\dots$
$\begin{cases} r_k = 0 \text{ si } q_k \text{ est pair, } 1 \text{ s'il est impair} \\ q_{k+1} = \left\lfloor \frac{q_k}{2} \right\rfloor \end{cases}$
$\dots$
$\begin{cases} r_n = 0 \text{ si } q_n \text{ est pair, } 1 \text{ s'il est impair} \\ q_{n+1} = \left\lfloor \frac{q_n}{2} \right\rfloor = 0 \end{cases}$

PROP : le nombre  $n$  de la décomposition ci-dessus est égal à  $\lceil \log_b(a) \rceil$  ; le nombre de chiffres de la décomposition en base  $b$  de  $a$  vaut donc  $\lceil \log_b(a) \rceil + 1$ .

D4

b) Une application de la décomposition binaire : l'addition égyptienne et l'exponentiation rapide.

La multiplication égyptienne des entiers  $>0$   $a = a_0$  et  $b = b_0$  consiste à effectuer l'algorithme :

$$\begin{cases} a_{k+1} = \left\lfloor \frac{a_k}{2} \right\rfloor \\ b_{k+1} = 2b_k \end{cases}$$

jusqu'à obtenir  $a_{n+1} = 0$  ; si l'on pose alors  $c_k = \begin{cases} b_k & \text{si } a_k \text{ est impair} \\ 0 & \text{si } a_k \text{ est pair} \end{cases}$ , on a alors :

$$ab = \sum_{k=0}^n c_k$$

Explication : si  $a = \frac{\text{base } 2}{r_n r_{n-1} \dots r_1 r_0} = \sum_{k=0}^n r_k 2^k$  est la décomposition binaire de  $a$ , on a en fait  $c_k = r_k b_k$ , donc

$$ab = \sum_{k=0}^n r_k 2^k b = \sum_{k=0}^n r_k b_k = \sum_{k=0}^n c_k$$

Exemple E1

L'exponentiation rapide de l'entier  $>0$   $b = b_0$  par l'entier  $>0$   $a = a_0$  consiste à effectuer l'algorithme :

$$\begin{cases} a_{k+1} = \left\lfloor \frac{a_k}{2} \right\rfloor \\ b_{k+1} = b_k^2 \end{cases}$$

jusqu'à obtenir  $a_{n+1} = 0$  ; si l'on pose alors  $c_k = \begin{cases} b_k & \text{si } a_k \text{ est impair} \\ 1 & \text{si } a_k \text{ est pair} \end{cases}$ , on a alors :

$$b^a = \prod_{k=0}^n c_k$$

Explication : si  $a = \frac{\text{base } 2}{r_n r_{n-1} \dots r_1 r_0} = \sum_{k=0}^n r_k 2^k$  est la décomposition binaire de  $a$ , on a en fait  $c_k = b_k^{r_k}$ , donc

$$b^a = b^{\sum_{k=0}^n r_k 2^k} = \prod_{k=0}^n b^{r_k 2^k} = \prod_{k=0}^n (b^{2^k})^{r_k} = \prod_{k=0}^n b_k^{r_k} = \prod_{k=0}^n c_k$$

Exemple E2

Le nom de cet algorithme vient de ce que dans une exponentiation normale de  $b$  par  $a$ , on effectue environ  $a$  multiplications, tandis que dans l'exponentiation rapide, on effectue environ  $\lceil \log_2(a) \rceil$  élévations au carrés et au plus  $\lceil \log_2(a) \rceil$  multiplications, et que

$$2^{\lceil \log_2(a) \rceil} \ll_{a \rightarrow +\infty} a$$

3) Congruences (hors programme).

a) Généralités.

Rappels : si  $(a, b, n) \in \mathbb{Z}^2 \times \mathbb{N}^*$   $a \equiv b \pmod{n}$  (ou  $\text{mod } n$ )  $\Leftrightarrow n \mid (b - a) \Leftrightarrow \exists k \in \mathbb{Z} / b = a + nk$

On a donc la relation très utile :

$$a \mid b \Leftrightarrow b \equiv 0 \pmod{a}$$

PROP : on peut aussi dire :  $a \equiv b \pmod{n} \Leftrightarrow \text{reste}(a, n) = \text{reste}(b, n)$ .

D5

PROP : en termes de congruences, le théorème de la division euclidienne peut s'énoncer : tout entier  $a$  est congru modulo un entier  $b > 0$  à un unique entier  $r$  appartenant à  $[[0, b - 1]]$  ; cela revient exactement à dire qu'il y a  $b - 1$  classes d'équivalence modulo  $b$  :  $b\mathbb{Z}$ ,  $b\mathbb{Z} + 1$ , ...,  $b\mathbb{Z} + b - 1$ .

b) Compatibilité des congruences avec l'addition et la multiplication.

TH : si  $(a, b, c, d, n) \in \mathbb{Z}^3 \times \mathbb{N}^*$  et  $\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases}$  alors  $a + c \equiv b + d [n]$  et  $ac \equiv bd [n]$  ; donc  $a^m \equiv b^m [n]$  pour tout naturel  $m$ .

D6

Applications A1 :

- $a^n - b^n$  est divisible par  $a - b$ , sans invoquer la formule de Bernoulli.
- $2^{6n+1} + 3^{2(n+1)}$  est divisible par 11 pour tout naturel  $n$ .
- $3 \cdot 5^{2n+1} + 2^{3n+1}$  est divisible par 17 pour tout naturel  $n$ .
- $3^{6n} - 2^{6n}$  est divisible par 35 pour tout naturel  $n \geq 1$ .
- une somme de deux carrés ne peut pas être de la forme  $4k - 1$ .

c) Applications aux critères de divisibilité en base 10.

PROP : un entier naturel est congru

- à son dernier chiffre en base 10, modulo 2 et 5.
- au nombre formé de ses deux derniers chiffres en base 10, modulo 4 et 25.
- à la somme des ses chiffres en base 10, modulo 3 et 9.
- à la somme alternée de ses chiffres  $\sum_{k=0}^n (-1)^k r_k$  en base 10, modulo 11.

D7

3) Nombres premiers entre eux, PGCD, PPCM.

a) Nombres premiers entre eux.

Pour  $a$  entier relatif on note  $D_a$  l'ensemble de ses diviseurs dans  $\mathbb{N}$ .

DEF : deux entiers relatifs  $a$  et  $b$  sont dits *premiers entre eux* ssi leur seul diviseur commun dans  $\mathbb{N}$  est 1 (i. e.  $D_a \cap D_b = \{1\}$ ).

TH de Bézout :  $a$  et  $b$  sont premiers entre eux si et seulement s'il existe deux entiers relatifs  $u$  et  $v$  tels que  $au + bv = 1$ .  
D8 (application du théorème des sous-groupe de  $\mathbb{Z}$ ).

COROLLAIRE : TH de Gauss : si  $a$  divise  $bc$  et  $a$  et  $b$  sont premiers entre eux, alors  $a$  divise  $c$ .

D9

b) PGCD.

DEF : le PGCD de deux entiers relatifs non nuls  $a$  et  $b$  est leur plus grand diviseur commun dans  $\mathbb{N}$  (i. e. plus grand élément pour la relation d'ordre habituelle de  $D_a \cap D_b$ );

Notation :  $PGCD(a, b)$  ou  $a \wedge b$ .

Pourquoi pgcd et non pgdc ? Peut-être un archaïsme plaçant les deux adjectifs avant le nom, ou une influence de l'anglais : GCD (greatest common divisor).

PROP 1 :  $a$  et  $b$  sont premiers entre eux ssi leur PGCD est 1.

D10

PROP 2 : un entier divise deux nombres ss'il divise leur PGCD ( $d \mid a$  et  $d \mid b \Leftrightarrow d \mid (a \wedge b)$ )

(par conséquent le PGCD est non seulement le plus grand pour la relation d'ordre usuelle mais aussi pour la relation de divisibilité).

D11

Coro : on peut poser que  $a \wedge 0 = 0 \wedge a = a$ .

PROP 3 : pour  $a, b, d$  entiers  $> 0$ ,  $d = a \wedge b$  ssi  $d$  divise  $a$  et  $b$  et  $a/d$  et  $b/d$  sont premiers entre eux.

D12

PROP 4 (conséquence du th de Bézout) :  $d = a \wedge b$  ssi  $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$  avec  $d \geq 0$ .

D13

c) Algorithme d'Euclide et application à l'obtention des coefficients de Bézout.

$\alpha$ ) Principe de l'algorithme d'Euclide basique (enseigné au collège), ou anthyphérèse :  $PGCD(a, b) = PGCD(\min(a, b), \max(a, b) - \min(a, b))$ .

Exemple :  $\boxed{PGCD(42,18)} = PGCD(18,24) = \boxed{PGCD(18,6)} = PGCD(6,12) = \boxed{PGCD(6,6)} = 6$

PROP : si on pose  $\begin{cases} a_0 = a \\ b_0 = b \end{cases}$  et  $\begin{cases} a_n = \min(a_{n-1}, b_{n-1}) \\ b_n = |a_{n-1} - b_{n-1}| \end{cases}$  on arrive toujours en un temps fini à un couple  $(a_n, b_n)$  où  $a_n = b_n$ , d'où l'obtention du PGCD du couple de départ.

D14

$\beta$ ) Principe de l'algorithme d'Euclide classique :  $PGCD(a, b) = PGCD(b, \text{quotient}(a, b))$ .

Exemple :  $PGCD(42,18) = PGCD(18,6) = PGCD(6,0) = 6$

PROP : si on pose  $\begin{cases} a_0 = a \\ b_0 = b \end{cases}$  et  $\begin{cases} a_n = b_n \\ b_n = \text{quotient}(a_n, b_n) \end{cases}$  on arrive toujours en un temps fini à un couple  $(a_n, b_n)$  où le  $b_n$  est nul, d'où l'obtention du PCGCD du couple de départ.

D15

$\gamma$ ) Obtention des coefficients de Bézout.

Exemple : on cherche deux entiers  $u$  et  $v$  tels que  $71u + 17v = \text{pgcd}(71, 17)$ .

On considère :

$X_1 = (1, 0, 71)$  et  $X_2 = (0, 1, 17)$  ; le quotient de 71 par 17 étant 4, on calcule

$X_3 = X_1 - 4X_2 = (1, -4, 3)$  ; le quotient de 17 par 3 étant 5, on calcule

$X_4 = X_2 - 5X_3 = (-5, 21, 2)$  ; le quotient de 3 par 2 étant 1, on calcule

$X_5 = X_3 - X_4 = (6, -25, 1)$  : 1 divisant 2, on s'arrête.

Résultat : le pgcd de 71 et 17 est 1 et  $1 = 6 \cdot 71 - 25 \cdot 17$  ; on a obtenu les coefficients de Bézout du couple  $(71, 17)$ .

Explication : cela vient du

LEMME : si  $a$  et  $b$  sont deux entiers, toute combinaison linéaire à coefficients entiers de triplets  $(u, v, w)$  vérifiant  $au + bv = w$  donne un triplet vérifiant la même relation

D16

4) Nombres premiers.

a) Généralités.

DEF :  $p \in \mathbb{N}$  est dit *premier* s'il possède exactement deux diviseurs dans  $\mathbb{N}$ , autrement dit s'il est différent de 1 et n'est divisible dans  $\mathbb{N}$  que par 1 et par lui-même. Un naturel  $\geq 2$  non premier est dit *composé*. On notera  $\mathbb{P}$  l'ensemble des nombres premiers.

PROP1 :  $n \in \mathbb{N}$  est composé  $\Leftrightarrow \exists d, d' \in \mathbb{N} / n = dd'$  avec  $2 \leq d, d' \leq n - 1$ .

D17

PROP2 : tout entier  $\geq 2$  est divisible par au moins un nombre premier .

THÉORÈME 1 :  $\mathbb{P}$  est infini (voir raisonnements par l'absurde).

b) Détermination des nombres premiers : critère et crible d'Ératosthène (-276 , -184).

Lemme : si  $n = dd'$  (avec  $n, d, d' \in \mathbb{N}^*$ ) alors  $d \leq \sqrt{n} \Leftrightarrow d' \geq \sqrt{n}$ .

THÉORÈME 2 (critère d'Ératosthène, pour déterminer si un entier donné est premier) :  
un entier  $n \geq 2$  est premier si et seulement s'il ne possède aucun diviseur premier dans  $[2, \sqrt{n}]$ .

D18

THÉORÈME 3 (algorithme du crible d'Ératosthène, pour déterminer la liste des nombres premiers entre 1 et  $n$ ) :

On part de la liste  $L_1 = (2, 3, \dots, n)$  et la liste  $L_k$  étant définie, on définit la liste  $L_{k+1}$  comme la liste obtenue en supprimant dans  $L_k$  tous les multiples stricts de son  $k$ -ième terme.

Alors, la première liste  $L_k$  dont le  $k$ -ième terme est  $\geq \sqrt{n}$  est la liste croissante des nombres premiers compris entre 1 et  $n$ .

D19

REM : le nombre d'étapes du crible d'Ératosthène est égal au nombre de nombres premiers entre 1 et  $\sqrt{n}$  ; on peut démontrer que ce nombre est  $\sim 2 \frac{\sqrt{n}}{\ln n}$ , ce qui explique pourquoi cet algorithme est très performant (cf info).

c) Décomposition en produit de facteurs premiers.

THÉOREME 4 : tout naturel  $\geq 2$  se décompose de manière unique en produit de nombres premiers ; l'unicité signifie précisément que si un même nombre est produit des éléments de 2 listes *croissantes* de nombres premiers, alors ces listes sont égales.

Unicité admise ; existence démontrée dans le cours sur les récurrences fortes.

DEF : un naturel  $a \geq 1$  et un nombre premier  $p$  étant donnés ; on appelle valuation en  $p$  de  $a$  le nombre  $\alpha_p(a)$  de fois que  $p$  intervient dans la décomposition de  $a$  en produit de facteurs premiers ; notation :  $\alpha_p(a)$  ; on a donc

$$a = \prod_{p \in \mathbb{P}} p^{\alpha_p(a)}$$

(on considère que le produit d'une infinité de "1" est égal à 1).

PROP : pour  $a, b, c \in \mathbb{N}^*$  on a :

a) $a = b \Leftrightarrow \forall p \in \mathbb{P} \alpha_p(a) = \alpha_p(b)$
b) $c = ab \Leftrightarrow \forall p \in \mathbb{P} \alpha_p(c) = \alpha_p(a) + \alpha_p(b)$
c) $a$ divise $b \Leftrightarrow \forall p \in \mathbb{P} \alpha_p(a) \leq \alpha_p(b)$
d) $d = \text{pgcd}(a, b) \Leftrightarrow \forall p \in \mathbb{P} \alpha_p(d) = \min(\alpha_p(a), \alpha_p(b))$
e) $m = \text{ppcm}(a, b) \Leftrightarrow \forall p \in \mathbb{P} \alpha_p(m) = \max(\alpha_p(a), \alpha_p(b))$
f) $a$ est un carré (parfait) $\Leftrightarrow \forall p \in \mathbb{P} \alpha_p(a)$ est pair
f') $a$ est une puissance $n$ -ième exacte $\Leftrightarrow \forall p \in \mathbb{P} n \mid \alpha_p(a)$

D20

CORO (de d) et e)) :

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = ab$$

D21

CORO (de f)) : si  $n$  est un naturel qui n'est pas un carré,  $\sqrt{n}$  est irrationnel.

CORO (de f')) : .....

D22