

Chapitre 10

Arithmétique

Sommaire

I	Divisibilité	95
1)	La propriété fondamentale	95
2)	La division euclidienne	96
3)	Congruences	96
4)	Diviseurs communs	96
II	Éléments premiers entre eux	97
1)	Théorème de Bézout	97
2)	Conséquences	98
III	Le plus grand diviseur commun	98
1)	Définition	98
2)	Propriétés	99
3)	Généralisation	100
IV	Le plus petit multiple commun	101
1)	Définition	101
2)	Propriétés	101
V	Nombres premiers, décomposition	102
1)	Définition	102
2)	Décomposition en facteurs premiers	103
3)	Notion de valuation p -adique	103
4)	Applications	104
VI	Solution des exercices	105

I DIVISIBILITÉ

1) La propriété fondamentale



Théorème 10.1

Toute partie de \mathbb{Z} non vide et minorée admet un plus petit élément.

Preuve : Soit A une partie de \mathbb{Z} non vide et minorée par un entier n_0 . Soit M l'ensemble des minorants de A , on a $n_0 \in M$, supposons que $n \in M \implies n+1 \in M$, alors d'après le principe de récurrence, $\forall n \in \mathbb{Z}, n \geq n_0 \implies n \in M$. Soit $p \in A$, $p \geq n_0$, donc $p+1 \in M$ ce qui entraîne que $p+1 \leq p$: absurde, donc il existe un entier n_1 tel que $n_1 \in M$ et $n_1+1 \notin M$, mais alors il existe un élément p_1 de A tel que $p_1 < n_1+1$, d'où $n_1 \leq p_1 < n_1+1$, ce qui entraîne $p_1 = n_1$, et donc $n_1 \in A$, nécessairement n_1 est le plus petit élément de A . \square



À retenir

- Toute partie non vide et majorée de \mathbb{Z} admet un plus grand élément. En effet, si A est non vide majorée, alors $-A = \{-a / a \in A\}$ est non vide minorée, donc $-A$ admet un plus petit élément $-n_0$, ce qui signifie que n_0 est le plus grand élément de A .
- Toute partie non vide de \mathbb{N} admet un plus petit élément (propriété fondamentale de \mathbb{N}).

2) La division euclidienne

**Théorème 10.2**

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, il existe un unique couple d'entiers (q, r) tel que $a = bq + r$ avec $0 \leq r < |b|$, q est appelé le quotient, et r le reste.

Preuve : Supposons $b > 0$: soit $B = \{b(n+1) / n \in \mathbb{Z}\}$, alors B est non majoré et non minoré, donc il existe un entier n_1 tel que $a < b(n_1 + 1)$ et il existe un entier n_2 tel que $b(n_2 + 1) < a$. Soit $A = \{n \in \mathbb{Z} / a < b(n+1)\}$, alors A est non vide ($n_1 \in A$) et minoré par n_2 , donc A admet un plus petit élément q , d'où $bq \leq a < b(q+1)$, en posant $r = a - bq$, on a $a = bq + r$ et $0 \leq r < b = |b|$.

Supposons $b < 0$: on applique ce qui précède à $-b > 0$, il existe un entier q et un entier r tels que $a = (-b)q + r = b(-q) + r$ avec $0 \leq r < -b = |b|$.

Montrons l'unicité : si $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$, alors $|r - r'| = |bq' - bq| = |b||q' - q| < |b|$, d'où $q' = q$ (ce sont des entiers) et donc $r' = r$. \square

**Définition 10.1**

Soient $a, b \in \mathbb{Z}$, on dit que b divise a lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = bk$. Notation : $b|a$.

Remarque 10.1 – On a ainsi défini une relation dans \mathbb{Z} , elle est réflexive, non symétrique, non antisymétrique, et transitive.

**Théorème 10.3**

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$, alors $b|a$ ssi le reste dans la division euclidienne de a par b est nul.

Preuve : Celle-ci est simple et laissée en exercice. \square

Notation : Soit $n \in \mathbb{Z}$, on note $n\mathbb{Z}$ l'ensemble des multiples de n , $n\mathbb{Z} = \{kn / k \in \mathbb{Z}\}$.

**Théorème 10.4**

- $b|a \iff a \in b\mathbb{Z}$.
- Si $a \neq 0$, alors $b|a \implies |b| \leq |a|$.
- $(a|b \text{ et } b|a) \iff a\mathbb{Z} = b\mathbb{Z} \iff a = \lambda b$ avec $\lambda = \pm 1$ [on dit que a et b sont associés].
- Si $b|a$ et $b|c$ alors $\forall u, v \in \mathbb{Z}, b|au + cv$.
- Si $nb|na$ et si $n \neq 0$, alors $b|a$.

3) Congruences

**Définition 10.2 (congruences)**

Soient $a, b, n \in \mathbb{Z}$, on dit que a est congru à b modulo n lorsque $n|a - b$. Notation : $a \equiv b \pmod{n}$.

**Théorème 10.5**

- La relation de congruence modulo n est une relation d'équivalence.
 - Soient $a, b, c, d, n \in \mathbb{Z}$, si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors :

$$ac \equiv bd \pmod{n} \text{ et } a + c \equiv b + d \pmod{n}.$$
- On dit que la relation de congruence est compatible avec les opérations.

Preuve : Celle-ci est simple et laissée en exercice. \square

☞ **Exemple :** Dans \mathbb{Z} , si $n = a_0 + 10a_1 + \dots + 10^p a_p$ (écriture décimale) alors $n \equiv a_0 + \dots + a_p \pmod{3}$ car $10^k \equiv 1 \pmod{3}$

4) Diviseurs communs

Définition 10.3 (diviseurs communs)

Pour $a \in \mathbb{Z}$, on note D_a l'ensemble des diviseurs de a . Si $a, b \in \mathbb{Z}$, on note $D_{a,b}$ l'ensemble des diviseurs communs à a et b , on a donc $D_{a,b} = D_a \cap D_b$, cet ensemble contient toujours ± 1 .

Remarque 10.2 –

- Pour tout élément $a \in \mathbb{Z}$, $\pm 1 \mid a$.
- Si $a \neq 0$, alors D_a est un ensemble fini, plus précisément $D_a \subset \llbracket -|a|; |a| \rrbracket$.
- $D_0 = \mathbb{Z}$, $D_{\pm 1} = \{\pm 1\}$.
- Si a et b sont dans \mathbb{Z} : $D_a = D_{|a|}$ (on en déduit que $D_{a,b} = D_{|a|,|b|}$).

Théorème 10.6

Soient $a, b, q, r \in \mathbb{Z}$, si $a = bq + r$, alors $D_{a,b} = D_{b,r}$.

Preuve : Si $d \in D_{a,b}$, alors $d \mid a$ et $d \mid b$ donc $d \mid a - bq$ i.e. $d \mid r$, donc $d \in D_{b,r}$.

Réciproquement, si $d \in D_{b,r}$, alors $d \mid b$ et $d \mid r$ donc $d \mid bq + r$ i.e. $d \mid a$, d'où $d \in D_{a,b}$. □

Application – Le théorème ci-dessus fournit un algorithme pour la recherche des diviseurs communs à a et b (entiers naturels) basé sur la division euclidienne : c'est l'**algorithme d'Euclide**¹, voici son principe :

On remarque que si $b = 0$ alors $D_{a,b} = D_a$. On peut supposer désormais que $b \neq 0$ et on cherche à calculer $D = D_{a,b}$:

Étape 1 : on effectue la division euclidienne de a par b , $a = bq_1 + r_1$ avec $0 \leq r_1 < b$. On a $D = D_{b,r_1}$, donc si $r_1 = 0$ alors $D = D_b$, sinon on passe :

Étape 2 : on effectue la division euclidienne de b par r_1 , $b = r_1q_2 + r_2$ avec $0 \leq r_2 < r_1$. On a $D = D_{r_1,r_2}$, donc si $r_2 = 0$ alors $D = D_{r_1}$, sinon on passe :

Étape 3 : on effectue la division euclidienne de r_1 par r_2 ; $r_1 = r_2q_3 + r_3$ avec $0 \leq r_3 < r_2$. On a $D = D_{r_2,r_3}$, donc si $r_3 = 0$ alors $D = D_{r_2}$, sinon on passe à l'étape 4...

La suite des restes obtenus est une suite strictement décroissante d'entiers positifs, elle est donc nécessairement finie, i.e. il existe un entier $n \geq 1$ tel que $r_n = 0$, l'ensemble cherché est donc $D = D_{r_{n-1}}$ (avec la convention $r_0 = b$).

À retenir

$D_{a,b} = D_r$ où r est le dernier reste non nul dans l'algorithme d'Euclide.

Exemple : Cherchons les diviseurs communs à $a = 336$ et $b = 210$

- on effectue la division de a par b : $336 = 1 \times 210 + 126$, donc $D_{a,b} = D_{210,126}$.
- on effectue la division de 210 par 126 : $210 = 1 \times 126 + 84$, donc $D_{a,b} = D_{210,126} = D_{126,84}$.
- on effectue la division de 126 par 84 : $126 = 1 \times 84 + 42$, donc $D_{a,b} = D_{84,42}$.
- on effectue la division de 84 par 42 : $84 = 2 \times 42 + 0$, donc $D_{a,b} = D_{42,0} = D_{42}$, c'est à dire :

$$D_{336,210} = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}.$$

II ÉLÉMENTS PREMIERS ENTRE EUX

1) Théorème de Bézout

Définition 10.4

Soient $a, b \in \mathbb{Z}$, on dit que a et b sont premiers entre eux (ou a est premier avec b) lorsque le seul diviseur commun positif est 1, i.e. $D_{a,b} = \{\pm 1\}$.

1. EUCLIDE (300 av. J.C. – 275 av. J.C. environ) : on ne sait pratiquement rien de sa vie, il était vraisemblablement grec. Son œuvre est colossale et son ouvrage fondamental « Les éléments » regroupe toutes les connaissances de l'époque, il faudra près de vingt siècles pour dépasser son œuvre.

Remarque 10.3 –

- Dire que a est premier avec b revient à dire que le dernier reste non nul dans l'algorithme d'Euclide est 1.
- Si a est premier avec b , alors au moins un des deux est non nul (sinon l'ensemble des diviseurs communs est \mathbb{Z}).
- a est premier avec a si et seulement si $a \pm 1$.

**Théorème 10.7 (théorème de Bézout²)**

Soient $a, b \in \mathbb{Z}$, alors a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Les entiers u et v sont appelés coefficients de Bézout (non uniques en général).

Preuve : Supposons que u et v existent et soit d un diviseur commun à a et b , alors $d \mid a$ et $d \mid b$, donc $d \mid au + bv$ i.e. $d \mid 1$, donc $d = \pm 1$ ce qui prouve que a et b sont premiers entre eux.

Réciproquement : si a est premier avec b . En appliquant l'algorithme d'Euclide on vérifie qu'à chaque étape le reste r_k peut se mettre sous la forme $r_k = au_k + bv_k$ avec u_k et v_k dans \mathbb{Z} (récurrence) (algorithme d'Euclide étendu), comme le dernier reste non nul est 1, il existe bien u et v dans \mathbb{Z} tels que $1 = au + bv$ (de plus on sait les calculer!). \square

☞ **Exemple :** $\forall n \in \mathbb{Z}$, n et $n + 1$ sont premiers entre eux, puisque $n + 1 - n = 1$.

2) Conséquences**Théorème 10.8**

Si a est premier avec b et si a est premier avec c , alors a est premier avec le produit bc . On en déduit que si a est premier avec c_1, \dots, c_n , alors a est premier avec le produit $c_1 \times \dots \times c_n$.

Preuve : Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$, il existe $p, q \in \mathbb{Z}$ tels que $ap + cq = 1$. On effectue le produit de ces deux relations, ce qui donne $a(ucq + uap + pbv) + bc(vq) = 1$, d'après le théorème de Bézout, a et bc sont premiers entre eux. Une simple récurrence sur n permet de démontrer la généralisation. \square

**Théorème 10.9**

Si a est premier avec c , si $a \mid b$ et si $c \mid b$, alors $ac \mid b$.

Preuve : Il existe $u, v \in \mathbb{Z}$ tels que $au + cv = 1$, on multiplie par b , ce qui donne : $bau + bcv = b$, or $c \mid b$ donc $ac \mid bau$, et $a \mid b$ donc $ac \mid bcv$, ce qui entraîne $ac \mid bau + bcv$ i.e. $ac \mid b$.

Remarquons que ce théorème est faux lorsque a et c ne sont pas premiers entre eux, par exemple : $2 \mid 12$ et $4 \mid 12$ mais $2 \times 4 = 8 \nmid 12$. \square

**Théorème 10.10 (théorème de Gauss)**

Si $a \mid bc$ et si a est premier avec c , alors $a \mid b$.

Preuve : Il existe $u, v \in \mathbb{Z}$ tels que $au + cv = 1$, on multiplie par b , ce qui donne $bau + bvc = b$, or $a \mid bc$ donc $a \mid bau + bvc$, i.e. $a \mid b$. \square

★ **Exercice 10.1** Résoudre dans \mathbb{Z} l'équation $17x + 12y = 3$.

III LE PLUS GRAND DIVISEUR COMMUN**1) Définition**

Soient $a, b \in \mathbb{Z}$ non tous deux nuls (i.e. $a \neq 0$ ou $b \neq 0$), on sait que $D_{a,b} = D_r$ où r est le dernier reste non nul dans l'algorithme d'Euclide, on voit que les diviseurs communs à a et b ont une valeur absolue inférieure ou égale à celle de r et donc r est le plus grand diviseur commun.

**Définition 10.5**

Soient $a, b \in \mathbb{Z}$ non tous deux nuls, on appelle pgcd de a et de b le plus grand diviseur commun. Notation : $\text{pgcd}(a, b)$ ou $a \wedge b$, c'est le dernier reste non nul dans l'algorithme d'Euclide.

2. BÉZOUT Étienne (1730 – 1783) : mathématicien français, l'un des précurseurs de la géométrie algébrique.

Remarque 10.4 – Il en découle que deux éléments a et b de \mathbb{Z} , non tous deux nuls, sont premiers entre eux si et seulement si $\text{pgcd}(a, b) = 1$.



Théorème 10.11 (Calcul pratique d'un pgcd)

Si $a, b \in \mathbb{Z}$ sont non tous deux nuls alors $\forall q \in \mathbb{Z}, \text{pgcd}(a, b) = \text{pgcd}(a - bq, b)$.

Preuve : Soit $r = a - bq$, on a $a = bq + r$ et on sait alors que $D_{a,b} = D_{b,r}$, le résultat en découle. \square

Listing 10.1: euclide pour a et b positifs

```

1 def pgcd(a, b):
2     A, B = a, b
3     while B != 0:
4         A, B = B, A%B
5     return(A) #dernier reste non nul

```

★Exercice 10.2

1/ Prouver la terminaison de l'algorithme.

2/ Montrer que l'on a l'invariant de boucle de boucle $P(k) = \langle \text{pgcd}(a, b) = \text{pgcd}(A_k, B_k) \rangle$.

3/ Conclure.

☞ **Exemple** : Soit à calculer $d = \text{pgcd}(3282, 1281)$:

– $3282 = 2 \times 1281 + 720$, donc $d = \text{pgcd}(1281, 720)$,

– $1281 = 1 \times 720 + 561$, donc $d = \text{pgcd}(720, 561)$,

– $720 = 1 \times 561 + 159$, donc $d = \text{pgcd}(561, 159)$,

– $561 = 3 \times 159 + 84$, donc $d = \text{pgcd}(159, 84)$,

– $159 = 1 \times 84 + 75$, donc $d = \text{pgcd}(84, 75)$,

– $84 = 1 \times 75 + 9$, donc $d = \text{pgcd}(75, 9)$,

– $75 = 8 \times 9 + 3$, donc $d = \text{pgcd}(9, 3)$,

– $9 = 3 \times 3 + 0$, donc $d = 3$.

2) Propriétés



Théorème 10.12 (caractérisations du pgcd)

Soient $a, b \in \mathbb{Z}$ non tous deux nuls, et soit $d \in \mathbb{N}^*$. On a alors :

• $d = \text{pgcd}(a, b) \iff d \mid a, d \mid b$ et $\exists u, v \in \mathbb{Z}$ tels que $au + bv = d$.

• $d = \text{pgcd}(a, b) \iff \exists u, v \in \mathbb{Z}$ premiers entre eux, tels que $a = du$ et $b = dv$.

Preuve : Pour le premier point : Si $d = \text{pgcd}(a, b)$, cela découle d l'algorithme d'Euclide étendu.

Si $d \mid a, d \mid b$ et $\exists u, v \in \mathbb{Z}$ tels que $au + bv = d$, alors d est diviseur commun à a et b , et la deuxième relation entraîne que tout diviseur commun à a et b est un diviseur de d , donc $d = \text{pgcd}(a, b)$ (d étant positif).

Pour le second point : Si $d = \text{pgcd}(a, b)$ alors il existe $u, v \in \mathbb{Z}$ tels que $a = du$ et $b = dv$, soit $k = u \wedge v$, alors kd divise a et b , donc $|kd| \leq |d|$ ce qui entraîne $|k| \leq 1$ et donc $k = 1$.

Si $a = du, b = dv$ avec $u \wedge v = 1$, alors d est un diviseur commun à a et b , d'après le théorème de Bézout, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha u + \beta v = 1$, d'où $d = \alpha a + \beta b$, et donc d'après le premier point, i.e. $d = a \wedge b$. \square



Théorème 10.13 (quelques propriétés du pgcd)

Soient $a, b \in \mathbb{Z}$ non tous deux nuls :

a) $\forall n \in \mathbb{Z}$, si $n \mid a$ et $n \mid b$, alors $n \mid \text{pgcd}(a, b)$.

b) $\forall k \in \mathbb{N}^*, \text{pgcd}(ka, kb) = k \text{pgcd}(a, b)$.

c) $\forall n \in \mathbb{N}, \text{pgcd}(a^n, b^n) = \text{pgcd}(a, b)^n$.

d) Si a et c sont premiers entre eux, alors $\text{pgcd}(a, bc) = \text{pgcd}(a, b)$.

Preuve : Pour le premier point : Soit $d = \text{pgcd}(a, b)$, alors $D_{a,b} = D_d$ donc tout diviseur commun à a et b est un diviseur de d .

Pour le deuxième point : soit $d = \text{pgcd}(a, b)$, alors il existe $u, v \in \mathbb{Z}$ premiers entre eux tels que $a = du$ et $b = dv$, d'où $ka = kdu$ et $kb = kdv$, donc $kd = \text{pgcd}(ka, kb)$.

Pour le troisième point : en reprenant les notations ci-dessus, $a^n = d^n u^n$ et $b^n = d^n v^n$, or u et v sont premiers entre eux, donc u^n et v^n aussi (conséquence du théorème de Bézout), par conséquent $d^n = \text{pgcd}(a^n, b^n)$.

Pour le dernier point : on reprend les notations ci-dessus, $a = du$ et $bc = dc v$ mais $u \mid a$ et a est premier avec c , donc u est premier avec c , d'où u est premier avec cv , et donc $d = \text{pgcd}(a, bc)$. \square

3) Généralisation

Soient a, b, c trois entiers non tous nuls, l'ensemble des diviseurs communs à a, b et c est :

$$D_{a,b,c} = D_a \cap D_b \cap D_c = (D_a \cap D_b) \cap D_c = D_a \cap (D_b \cap D_c)$$

or on sait que $D_a \cap D_b = D_{a \wedge b}$, donc $D_{a,b,c} = D_{(a \wedge b) \wedge c} = D_{a \wedge (b \wedge c)}$. Ces deux entiers étant strictement positifs, on a $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ et ce nombre est le plus grand diviseur positif commun à a, b et c . Par définition ce nombre est le pgcd de a, b et c , on le note : $\text{pgcd}(a, b, c)$.



Théorème 10.14 (associativité du pgcd)

Soient a, b, c trois entiers avec b non nul, alors $\text{pgcd}(a, b, c) = (a \wedge b) \wedge c = a \wedge (b \wedge c)$.



À retenir

L'associativité du pgcd permet de ramener le calcul au cas de deux entiers.

Notons $d' = a \wedge b$ et $d = \text{pgcd}(a, b, c)$, alors $d = d' \wedge c$, donc il existe deux entiers u' et w tels que $d = d'u' + cw$, de même, il existe deux entiers α et β tels que $d' = \alpha a + \beta b$, d'où en remplaçant, $d = \alpha \alpha u' + \beta \beta u' + cw = au + bv + cw$ avec $u, v, w \in \mathbb{Z}$.

Réciproquement, si d est un diviseur commun positif, et si $d = au + bv + cw$, alors il est facile de voir que tout diviseur commun à a, b et c est un diviseur de d et donc $d = \text{pgcd}(a, b, c)$, d'où le théorème :



Théorème 10.15

Soient a, b, c trois entiers non tous nuls et $d \in \mathbb{N}^*$, alors :

$$d = \text{pgcd}(a, b, c) \iff d \in D_{a,b,c} \text{ et } \exists u, v, w \in \mathbb{Z}, d = au + bv + cw.$$



Définition 10.6

Soient a, b, c trois entiers non tous nuls, on dira que ces trois nombres sont :

- **premiers entre eux dans leur ensemble** lorsque $\text{pgcd}(a, b, c) = 1$.
- **premiers entre eux deux à deux** lorsque $\text{pgcd}(a, b) = \text{pgcd}(b, c) = \text{pgcd}(a, c) = 1$.



Attention!

Les deux notions ne sont pas équivalentes, **la deuxième entraîne la première mais la réciproque est fautive** comme le montre l'exemple suivant :

$$\text{pgcd}(6, 15, 20) = 1 \text{ mais } \text{pgcd}(6, 15) = 3, \text{pgcd}(6, 20) = 2 \text{ et } \text{pgcd}(15, 20) = 5.$$

Il découle du théorème précédent :



Théorème 10.16 (de Bézout)

Soient a, b, c trois entiers non tous nuls, alors a, b et c sont premiers entre eux dans leur ensemble si et seulement si :

$$\exists u, v, w \in \mathbb{Z}, au + bv + cw = 1.$$



Théorème 10.17 (caractérisation)

Soient a, b, c trois entiers non tous nuls et $d \in \mathbb{N}^*$, alors :

$$d = \text{pgcd}(a, b, c) \iff \exists u, v, w \in \mathbb{Z}, a = du, b = dv \text{ et } c = dw \text{ avec } \text{pgcd}(u, v, w) = 1.$$

Preuve : Si $d = \text{pgcd}(a, b, c)$ alors il existe $\exists u, v, w \in \mathbb{Z}, a = du, b = dv$ et $c = dw$. Il existe également des entiers α, β et γ tels que $1 = \alpha u + \beta v + \gamma c$ d'où $1 = \alpha u + \beta v + \gamma c$ et donc $\text{pgcd}(u, v, w) = 1$.

Réciproquement, si $a = du, b = dv$ et $c = dw$ avec $\text{pgcd}(u, v, w) = 1$. Il existe des entiers α, β et γ tels que $1 = \alpha u + \beta v + \gamma w$, en multipliant par d il vient alors que $d = \alpha a + \beta b + \gamma c$, ce qui entraîne que $d = \text{pgcd}(a, b, c)$ (car $d \in \mathbb{N}^*$ et $d \in D_{a,b,c}$). \square

Remarque 10.5 – Nous avons étendu la notion de pgcd à trois entiers, mais on pourrait l'étendre de la même manière à n entiers.

IV LE PLUS PETIT MULTIPLE COMMUN

1) Définition



Théorème 10.18

Si a et b sont non nuls, il existe un unique élément m positif dans \mathbb{Z} tel que $(a\mathbb{Z}) \cap (b\mathbb{Z}) = m\mathbb{Z}$.

Preuve : $a\mathbb{Z} \cap b\mathbb{Z}$ contient $|ab| > 0$, on note m le plus petit élément strictement positif dans $a\mathbb{Z} \cap b\mathbb{Z}$, alors il est facile de voir que $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$. Si $p \in a\mathbb{Z} \cap b\mathbb{Z}$, on effectue la division de p par m , $p = mq + r$ avec $0 \leq r < m$, d'où $r = p - mq$, on vérifie alors que r est aussi dans $a\mathbb{Z} \cap b\mathbb{Z}$ (car a et b divisent p et m donc $p - mq$). Si $r > 0$ alors $r \geq m$ car m est le plus petit élément strictement positif dans $a\mathbb{Z} \cap b\mathbb{Z}$, ceci est absurde, donc $r = 0$ et $p = mq$, d'où $a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$, et finalement on a bien l'inégalité.

Si $m'\mathbb{Z} = m\mathbb{Z}$ avec $m' > 0$, alors m et m' se divisent mutuellement, d'où $m = m'$. \square

Il découle de ce théorème que c est un multiple commun à a et b si et seulement si $c \in (a\mathbb{Z}) \cap (b\mathbb{Z})$, ce qui équivaut à $c \in m\mathbb{Z}$, c'est à dire $m \mid c$. Ceci entraîne en particulier : $m \leq |c|$.



Définition 10.7

Soit $a, b \in \mathbb{Z}$, non nuls, et soit $m \in \mathbb{N}^*$, on dit que m est le ppcm de a et b lorsque $(a\mathbb{Z}) \cap (b\mathbb{Z}) = m\mathbb{Z}$.

Notation : $m = \text{ppcm}(a, b)$ ou encore $m = a \vee b$.



Théorème 10.19 (caractérisation du ppcm)

Soient $a, b \in \mathbb{Z}$, non nuls, et soit $m \in \mathbb{N}^*$ alors :

$$m = \text{ppcm}(a, b) \iff \exists u, v \in \mathbb{Z} \text{ premiers entre eux; tels que } m = au = bv.$$

Preuve : On suppose $a, b \in \mathbb{Z}$, non nuls. Si $m = \text{ppcm}(a, b)$: alors $a \mid m$ et $b \mid m$. Donc il existe $u, v \in \mathbb{Z}$ tels que $m = au = bv$, soit $d = \text{pgcd}(u, v)$ alors il existe $\alpha, \beta \in \mathbb{Z}$ premiers entre eux tels que $u = d\alpha$ et $v = d\beta$, d'où $m = ad\alpha = bd\beta$, mais alors $m' = a\alpha = b\beta$ est un multiple commun à a et b donc $|m| \leq |m'|$ ce qui entraîne $d = 1$.

Si $\exists u, v \in \mathbb{Z}$ premiers entre eux tels que $m = au = bv$, alors $a \mid m$ et $b \mid m$, il existe α, β tels que $u\alpha + v\beta = 1$, soit m' un multiple commun non nul, alors $m' = m'u\alpha + m'v\beta$, on en déduit que $m \mid m'$ et donc $|m| \leq |m'|$, ce qui prouve que $m = \text{ppcm}(a, b)$. \square

2) Propriétés



Théorème 10.20

Soient $a, b \in \mathbb{Z}$, non nuls :

- $\forall n \in \mathbb{Z}$, si $a \mid n$ et $b \mid n$ alors $\text{ppcm}(a, b) \mid n$.
- Si a et b sont premiers entre eux, alors $\text{ppcm}(a, b) = |ab|$.
- $\forall k \in \mathbb{N}$, non nul, $\text{ppcm}(ka, kb) = k\text{ppcm}(a, b)$.
- $\text{ppcm}(a, b) \times \text{pgcd}(a, b) = |ab|$.
- $\forall n \in \mathbb{N}$, $\text{ppcm}(a^n, b^n) = \text{ppcm}(a, b)^n$.

Preuve : Pour le deuxième point : a et b sont premiers entre eux, alors $ab = ba$ par conséquent $\text{ppcm}(a, b) = ab$ d'après le théorème précédent.

Pour le troisième point : soit $m = \text{ppcm}(a, b)$, alors $m = au = bv$ avec u et v premiers entre eux, d'où $km = kau = kbv$ et donc $km = \text{ppcm}(ka, kb)$.

Pour le quatrième point : soit $m = \text{ppcm}(a, b)$ et $d = \text{pgcd}(a, b)$, il existe u et v premiers entre eux tels que $a = dv$ et $b = du$, or $au = bv$ donc $m = au = bv$ par conséquent $md = adu = ab$.

Pour le cinquième point : soit $m = \text{ppcm}(a, b)$ on a $m = au = bv$ avec u et v premiers entre eux, donc $m^n = a^n u^n = b^n v^n$ avec u^n et v^n premiers entre eux, donc $m^n = \text{ppcm}(a^n, b^n)$. \square

V NOMBRES PREMIERS, DÉCOMPOSITION

1) Définition



Définition 10.8

Un entier $p \in \mathbb{Z}$ est dit **premier** lorsque $p \geq 2$, et que ses seuls diviseurs positifs sont 1 et p . L'ensemble des nombres premiers est noté \mathcal{P} .

Exemples :

- 2, 3, 5, 7, 11, 13, 17, 19, 23, ... sont des nombres premiers.
- Les nombres de *Fermat*³ : $F_n = 2^{2^n} + 1$ sont premiers pour $n = 0, 1, 2, 3, 4$ mais pas pour $n = 5$, car $F_5 = 641 \times 6700417$.
- Les nombres de *Mersennes*⁴ : $M_p = 2^p - 1$ où $p \in \mathcal{P}$, sont premiers pour $p = 2, 3, 5, 7, 127, \dots$ mais pas pour $p = 11$, car $M_{11} = 23 \times 89$.

★Exercice 10.3

1/ Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$, montrer que $a - b \mid a^n - b^n$. Si n est impair, montrer que $a + b \mid a^n + b^n$.

2/ Montrer que si $2^p + 1$ est un nombre premier alors p est une puissance de 2.

3/ Montrer que si $2^p - 1$ est un nombre premier, alors p est un nombre premier.

Propriétés élémentaires :

a) Si p est premier, alors $\forall n \in \mathbb{Z}$, soit $p \mid n$, soit $\text{pgcd}(n, p) = 1$.

Preuve : Soit $d = \text{pgcd}(p, n)$, alors $d \mid p$ donc $d = 1$ ou $d = p$, mais p ne divise pas n , donc $d \neq p$, i.e. $d = 1$. □

b) Si $n \geq 2$, alors n possède au moins un diviseur premier.

Preuve : Soit $B = \{d \mid d \mid n \text{ et } d \neq 1\}$, alors B est une partie de \mathbb{N} non vide ($|n| \in B$), soit p un diviseur de n avec $|p| \in B$ **minimal**, si $d \mid p$ avec d positif et $d \neq 1$, alors $d \mid n$ et donc $|d| \in B$, d'où $|d| \geq |p|$, or $d \mid p$, donc $|d| \leq |p|$ et finalement $|d| = |p|$, d'où $d = p$ et donc p est premier. □

c) L'ensemble \mathcal{P} est infini.

Preuve : Si \mathcal{P} est fini, alors $\mathcal{P} = \{p_1, \dots, p_n\}$, posons $N = 1 + p_1 \times \dots \times p_n$, alors $N > 1$, donc N admet au moins un diviseur premier q , comme $q \in \mathcal{P}$, on a $q \mid p_1 \times \dots \times p_n$, et comme $q \mid N$, on a $q \mid 1$ ce qui est absurde, donc \mathcal{P} est infini. □

d) Si p est premier et si $p \mid nm$, alors $p \mid n$ ou $p \mid m$.

Preuve : Supposons que p ne divise pas n , alors $n \notin p\mathbb{Z}$ donc $\text{pgcd}(p, n) = 1$ et par conséquent $p \mid m$ (d'après le théorème de *Gauss*). □

e) Si $n > 1$ n'a pas de diviseur autre que 1 dans l'intervalle $[1; \sqrt{n}]$, alors n est premier.

Preuve : Si n est non premier alors on peut écrire $n = pq$ avec $p > 1$ et $q > 1$. Si les deux étaient strictement supérieurs à \sqrt{n} alors on aurait $pq > n$ ce qui est absurde, donc un des deux est dans $[1; \sqrt{n}]$. Le résultat s'en déduit par contraposée. □

f) Si p est premier, alors $\forall k \in \llbracket 1; p-1 \rrbracket$, $p \mid \binom{p}{k}$. On en déduit que pour tout entier a et b , on a $(a+b)^p \equiv a^p + b^p \pmod{p}$.


Preuve : On a $k \binom{p}{k} = p \binom{p-1}{k-1}$ qui est donc divisible par p , mais comme $k \in \llbracket 1; p-1 \rrbracket$, p est premier avec k , par conséquent, d'après le théorème de *Gauss*, $p \mid \binom{p}{k}$. Pour le second point, on développe le binôme. □

Compléments : Soit $(p_n)_{n \geq 1}$ la suite strictement croissante des nombres premiers, la répartition de ces nombres encore aujourd'hui mal connue, cependant on a les quelques résultats suivants :

- Tout segment de la forme $\llbracket n; 2n \rrbracket$ contient au moins un nombre premier (théorème de *Bertrand*).
- Si $a, b \in \mathbb{N}^*$ sont premiers entre eux, alors il existe une infinité de nombre premiers de la forme $an + b$ (théorème de *Dirichlet*).
- $p_n \underset{+\infty}{\sim} n \ln(n)$ (théorème de *Hadamard*).

3. *FERMAT Pierre De* (1601 – 1665) : mathématicien amateur (éclairé!) l'un des plus féconds de son époque mais qui faisait peu de démonstrations et publiait peu.

4. *MERSENNE Marin* (1588 – 1648) : moine français qui entretenait une correspondance suivie avec les mathématiciens de son époque.

 **Théorème 10.21 (petit théorème de Fermat)**

Si p est un nombre premier, alors pour tout entier n on a $n^p \equiv n \pmod{p}$. Et si $n \notin p\mathbb{Z}$, alors $n^{p-1} \equiv 1 \pmod{p}$.

Preuve : Pour $n \in \mathbb{N}$ on fait une récurrence : la propriété est vraie au rang 0, supposons la vraie au rang n , alors $(n+1)^p \equiv n^p + 1 \pmod{p}$, en appliquant l'hypothèse de récurrence, on a $(n+1)^p \equiv n+1 \pmod{p}$.

On remarque ensuite que $(-1)^p \equiv -1 \pmod{p}$ car soit $p=2$, soit p est premier impair, on en déduit que $(-n)^p \equiv -n \pmod{p}$. On a donc pour tout entier n , $p \mid n^p - n = n(n^{p-1} - 1)$, si p ne divise pas n alors p est premier avec n , donc $p \mid n^{p-1} - 1$, c'est à dire $n^{p-1} \equiv 1 \pmod{p}$. □

2) Décomposition en facteurs premiers


 **Théorème 10.22 (décomposition en produit de facteurs premiers)**

Tout élément $n \in \mathbb{Z}$, autre que ± 1 , est un produit de nombres premiers. Plus précisément, il existe $r \geq 1$, il existe $p_1, \dots, p_r \in \mathcal{P}$ (distincts), il existe des entiers $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$, il existe $\lambda \in \{-1; 1\}$ tels que :

$$n = \lambda \times p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}.$$

Preuve : On a $n = \lambda \times |n|$ avec $\lambda = \pm 1$. On se ramène ainsi au cas où n est positif.

Par récurrence sur n : pour $n=2$ il n'y a rien à montrer car 2 est premier. Supposons le théorème démontré jusqu'au rang $n \geq 2$, alors $n+1$ admet au moins un diviseur premier p , donc $n+1 = pk$, si $k=1$ alors $n+1$ est premier, sinon k est un produit de facteurs premiers (HR), donc $n+1$ aussi. □

 **Théorème 10.23 (unicité de la décomposition)**

Si $n \in \mathbb{Z}$ s'écrit sous la forme :

$$n = \lambda \times p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r} = \mu \times q_1^{\beta_1} \times \dots \times q_s^{\beta_s},$$


avec $p_1, \dots, p_r \in \mathcal{P}$ (distincts), $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$, $q_1, \dots, q_s \in \mathcal{P}$ (distincts), $\beta_1, \dots, \beta_s \in \mathbb{N}^*$, et $\lambda, \mu \in \{-1; 1\}$ alors $r = s$, $\lambda = \mu$ et il existe une permutation σ de $\llbracket 1; r \rrbracket$ telle que pour $i \in \llbracket 1; r \rrbracket$, $p_i = q_{\sigma(i)}$, $\alpha_i = \beta_{\sigma(i)}$. La décomposition est unique (à l'ordre près).

Preuve : Si $p_1 \notin \{q_1, \dots, q_s\}$, alors p_1 est premier avec q_1, \dots, q_s , donc p_1 est premier avec $q_1^{\beta_1} \times \dots \times q_s^{\beta_s}$, i.e. p_1 est premier avec n , ce qui est absurde puisque $p_1 \mid n$, donc $p_1 \in \{q_1, \dots, q_s\}$. Finalement on a $\{p_1, \dots, p_r\} \subset \{q_1, \dots, q_s\}$ et par symétrie on a l'égalité des deux ensembles, donc $r = s$. Quitte à permuter les indices que la famille (q_i) , on peut supposer que $p_1 = q_1, \dots, p_r = q_r$.

Le théorème de Gauss entraîne que $p_k^{\alpha_k} \mid p_k^{\beta_k}$, donc $\alpha_k \leq \beta_k$, par symétrie on a $\beta_k \leq \alpha_k$, et donc $\alpha_k = \beta_k$, ce qui termine la preuve. □

3) Notion de valuation p -adique

Si n est un entier naturel non nul et p un nombre premier, alors l'ensemble $\{k \in \mathbb{N} \mid p^k \mid n\}$ est non vide (contient 0) et majoré par n (on peut montrer par récurrence que $p^n \geq n$), cet ensemble admet donc un maximum :

 **Définition 10.9**

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$ on appelle valuation p -adique de n , notée $v_p(n)$, le plus grand entier k tel que $p^k \mid n$. La définition s'étend à \mathbb{Z} , en posant $v_p(-n) = v_p(n)$ si $n < 0$ et $v_p(0) = +\infty$.

Remarque 10.6 :

- $v_p(n) = k \iff p^k \mid n \text{ et } p^{k+1} \nmid n \iff \exists q \in \mathbb{N}, n = p^k q \text{ avec } p \wedge q = 1.$
- $v_p(n) \geq 1 \iff p \mid n$, auquel cas $v_p(n)$ est la puissance de p dans la décomposition de n en facteurs premiers.
- $\{k \in \mathbb{N} \mid p^k \mid n\} = \llbracket 0; v_p(n) \rrbracket.$

 **À retenir**

Pour tout entier $n \geq 2$, la décomposition de n en produit de facteurs premiers s'écrit : $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$.

En effet, seul un nombre fini de valuations sont non nulles (les autres donnent un facteur égal à 1).



Théorème 10.24 (Propriétés)

$\forall n, m \in \mathbb{Z}$, on a :

- a) $\forall p \in \mathcal{P}, v_p(nm) = v_p(n) + v_p(m)$.
- b) $\forall p \in \mathcal{P}, v_p(n + m) \geq \min(v_p(n); v_p(m))$.
- c) $n \mid m \iff \forall p \in \mathcal{P}, v_p(n) \leq v_p(m)$.
- d) Si n et m sont non nuls alors $\forall p \in \mathcal{P}$:

$$v_p(n \wedge m) = \min(v_p(n); v_p(m)) \text{ et } v_p(n \vee m) = \max(v_p(n); v_p(m)).$$

Preuve :

- a) Si un des deux est nul, c'est évident. Supposons n et m non nuls, soit $n = p^k q$ avec $p \wedge q = 1$ et $m = p^{k'} q'$ avec $p \wedge q' = 1$, d'où $nm = p^{k+k'} qq'$ et $p \wedge (qq') = 1$, donc $v_p(nm) = k + k'$.
- b) Si un des deux est nul, c'est évident. Supposons n et m non nuls, et avec les mêmes notations, supposons $k \leq k'$, alors $n + m = p^k [q + p^{k'-k} q']$ donc $v_p(n + m) \geq k$. On remarque qu'il y a égalité lorsque $k \neq k'$.
- c) Si $m = 0$ c'est évident, supposons $m \neq 0$ et $n \mid m$, alors pour tout premier p , $\{k \in \mathbb{N} \mid p^k \mid n\} \subset \{k \in \mathbb{N} \mid p^k \mid m\}$ donc $v_p(n) \leq v_p(m)$. La réciproque est évidente.
- d) Soit $d = n \wedge m$ alors $v_p(d) \leq v_p(n)$ et $v_p(d) \leq v_p(m)$, donc $v_p(d) \leq \min(v_p(n); v_p(m))$. D'autre part $p^{\min(v_p(n); v_p(m))}$ divise n et m donc divise d d'où $\min(v_p(n); v_p(m)) \leq v_p(d)$, par conséquent $\min(v_p(n); v_p(m)) = v_p(d)$. Pour le ppccm on peut utiliser le fait que $(n \wedge m)(n \vee m) = |nm|$ et donc $v_p(n \vee m) = v_p(nm) - v_p(n \wedge m) = v_p(n) + v_p(m) - \min(v_p(n); v_p(m)) = \max(v_p(n); v_p(m))$.

□



À retenir : formules du pgcd et du ppccm

Il découle du théorème ci-dessus que :

$$\text{pgcd}(n, m) = \prod_{p \in \mathcal{P}} p^{\min(v_p(n); v_p(m))} \text{ et } \text{ppccm}(n, m) = \prod_{p \in \mathcal{P}} p^{\max(v_p(n); v_p(m))}.$$

★ **Exercice 10.4** Soient n et m deux naturels non nuls, premiers entre eux, tels que le produit nm est un carré, montrer que n et m sont des carrés.

4) Applications

- Si $n \neq \pm 1$, alors la décomposition de n en produit de facteurs premiers permet de trouver tous les diviseurs de n .
En effet : Si $n = \lambda \times p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$, soit d est un diviseur positif de n , si p est un diviseur premier de d , alors p est un diviseur premier de n , donc $p \in \{p_1, \dots, p_r\}$, donc d s'écrit sous la forme :

$$d = p_1^{\beta_1} \times \dots \times p_r^{\beta_r} \text{ avec } 0 \leq \beta_k \leq \alpha_k$$

- Si $n, m \notin \{-1; 1\}$, alors à partir de leur décomposition en produit de facteurs premiers, on peut calculer $\text{pgcd}(n, m) = \prod_{p \in \mathcal{P}} p^{\min(v_p(n); v_p(m))}$ et $\text{ppccm}(n, m) = \prod_{p \in \mathcal{P}} p^{\max(v_p(n); v_p(m))}$. Plus précisément : Si $n = \lambda \times p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ et $m = \mu \times q_1^{\beta_1} \times \dots \times q_s^{\beta_s}$, alors les diviseurs premiers communs à n et m doivent appartenir à $\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\}$, d'où la discussion :
 - $\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\} = \emptyset$, alors n et m sont premiers entre eux, i.e. $\text{pgcd}(n, m) = 1$ et donc $\text{ppccm}(n, m) = |nm|$.
 - $\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\} = \{v_1, \dots, v_t\}$, alors quitte à changer la numérotation, on peut supposer que $p_1 = q_1 = v_1, \dots, p_t = q_t = v_t$ sont les diviseurs premiers communs à n et m .

$$\text{pgcd}(n, m) = v_1^{k_1} \times \dots \times v_t^{k_t} \text{ avec } k_i = \min(\alpha_i, \beta_i) \text{ pour } i \in \llbracket 1; t \rrbracket.$$

Et :

$$\text{ppccm}(n, m) = v_1^{k_1} \times \dots \times v_t^{k_t} \times p_{t+1}^{\alpha_{t+1}} \times \dots \times p_r^{\alpha_r} \times q_{t+1}^{\beta_{t+1}} \times \dots \times q_s^{\beta_s} \text{ avec } k_i = \max(\alpha_i, \beta_i) \text{ pour } i \in \llbracket 1; t \rrbracket.$$

☞ **Exemple :** $336 = 2^4 \times 3 \times 7$ et $420 = 2^2 \times 3 \times 5 \times 7$, donc $\text{pgcd}(336, 420) = 2^2 \times 3 \times 7 = 84$, et $\text{ppccm}(336, 420) = 2^4 \times 3 \times 5 \times 7$.

VI SOLUTION DES EXERCICES

Solution 10.1 $a = 17$ et $b = 12$ sont premiers entre eux, appliquons l'algorithme d'Euclide :

$$a = b \times 1 + 5 \text{ d'où } r_1 = 5 = a - b$$

$$b = r_1 \times 2 + 2, \text{ d'où } r_2 = 2 = b - 2r_1 = b - 2(a - b) = -2a + 3b$$

$$r_1 = r_2 \times 2 + 1, \text{ d'où } r_3 = 1 = r_1 - 2r_2 = a - b + 4a - 6b = 5a - 7b$$

On a ainsi une relation de Bézout entre a et b , on en déduit une solution particulière en multipliant par 3 : $15a - 21b = 3$, donc $(x_0 = 15, y_0 = -21)$ est une solution particulière.

L'équation équivaut alors à $a(x - x_0) = b(y_0 - y)$, d'après le théorème de Gauss, a et b étant premiers entre eux, on a $b \mid x - x_0$ et $a \mid y_0 - y$, i.e. $x = x_0 + bk$ et $y = y_0 - bk'$, en reportant dans la relation on voit que $k = k'$ et donc les solutions sont les couples $(x_0 + bk, y_0 - ak)$ avec $k \in \mathbb{Z}$.

Solution 10.2

1/ À l'itération 0, on a $B_0 = b \in \mathbb{N}$. Si la boucle ne se termine jamais, alors on a une suite B_i de nombres non nuls. À l'itération $i + 1$, on a $A_{i+1} = B_i$ et B_{i+1} est le reste de la division de A_i par B_i , on en déduit par récurrence sur i , que (B_i) est une suite d'entiers positifs ($B_0 = b \in \mathbb{N}$) et strictement décroissante car $B_{i+1} < B_i$, ce qui est absurde, donc la boucle while se termine.

2/ Montrons l'invariant de boucle $P(i)$: $\text{pgcd}(a, b) = \text{pgcd}(A_i, B_i)$, par récurrence sur i , au rang 0, on a $A_0 = a$ et $B_0 = b$, $P(0)$ est donc vraie. Supposons $P(i)$ vraie et qu'il y a une itération $i + 1$, donc $B_i \neq 0$, à l'itération $i + 1$ on a $A_{i+1} = B_i$, et $A_i = B_i Q_i + B_{i+1}$ (division euclidienne de A_i par B_i), donc $\text{pgcd}(A_i, B_i) = \text{pgcd}(B_i, B_{i+1}) = \text{pgcd}(A_{i+1}, B_{i+1})$, ce qui montre $P(i + 1)$.

3/ Soit n le nombre d'itérations, à l'issue de l'itération n , on a $\text{pgcd}(a, b) = \text{pgcd}(A_n, B_n)$ (invariant), et comme il n'y a pas d'itération $n + 1$ cela signifie que $B_n = 0$, finalement $\text{pgcd}(a, b) = \text{pgcd}(A_n, 0) = A_n$. La valeur de la variable A qui est renvoyée est bien le pgcd cherché.

Solution 10.3

1/ $a \equiv b \pmod{a - b}$ d'où $a^n \equiv b^n \pmod{a - b}$, c'est à dire $a - b \mid a^n - b^n$.

$a \equiv -b \pmod{a + b}$ d'où $a^n \equiv (-b)^n \pmod{a + b}$, si n est impair alors $a^n \equiv -b^n \pmod{a + b}$, et donc $a + b \mid a^n + b^n$.

2/ Soit $N = 2^p + 1$ un nombre premier, on peut écrire $p = 2^r q$ avec q impair (r est valuation 2-adique de p), on a alors $N = 2^{2^r q} + 1 = \left(2^{2^r}\right)^q + 1^q$, q étant impair, N est divisible par $2^{2^r} + 1$, ce nombre est plus grand que 1 et N est premier, donc $2^{2^r} + 1 = N = 2^p + 1$, ce qui entraîne $p = 2^r$ (et donc $q = 1$).

3/ Soit $N = 2^p - 1$ un nombre premier, soit d un diviseur positif de p , on peut écrire $p = dq$ avec $q \in \mathbb{N}$, on a alors $N = 2^{dq} - 1 = 2^{d^q} - 1^q$, donc N est divisible par $2^d - 1$, or N est premier, donc $2^d - 1 = 1$ ou bien $2^d - 1 = N = 2^p - 1$, ce qui entraîne $d = 1$ ou $d = p$, donc p est premier.

Solution 10.4 Soit p un nombre premier, comme $n \wedge m = 1$, on a $v_p(n \wedge m) = 0$, or $v_p(n \wedge m) = \min(v_p(n); v_p(m))$, on a donc $v_p(n) = 0$ ou $v_p(m) = 0$, d'autre part, nm étant un carré d'entier, $v_p(nm)$ est pair, or $v_p(nm) = v_p(n) + v_p(m)$ et une des deux valuations est nulle, donc l'autre est forcément paire. Finalement, pour tout premier p , $v_p(n)$ est pair et $v_p(m)$ est pair, donc n et m sont des carrés d'entiers.