Arithmétique

MPSI-1 Prytanée National Militaire

Pascal Delahaye : D'après le cours d'Alain Soyeur

20 janvier 2011

1 La division euclidienne.

THÉORÈME FONDAMENTAL 1 : **Division euclidienne**
Soient deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.

Alors : $\exists!\ (q,\ r) \in \mathbb{Z}^2$ tels que : $\boxed{a = qb + r \quad \text{ET} \quad 0 \leq r < b}$

L'entier q est appelé le *quotient* et r est appelé le *reste* de la division euclidienne de a par b.

Preuve 1 :

1. On commence par une analyse qui permet de conclure à l'unicité de q et r : $\left\{ \begin{array}{l} q = E(a/b) \\ r = a - bq \end{array} \right.$.
2. Réciproquement, on montre que ces deux valeurs conviennent bien !

Dessin

Division euclidienne

Remarque 1. Effectuer la division euclidienne de a par b signifie déterminer les entiers q et r tels que $\left\{ \begin{array}{l} a = bq + r \\ 0 \leq r < b \end{array} \right.$.

`Exemple` 1. La division euclidienne permet de démontrer que les sous-groupes de $\mathbb{Z}$ sont de la forme $m\mathbb{Z}$ avec $m \in \mathbb{N}$

DÉFINITION 1 : **La relation "divise"**
Soit $(a,\ b) \in \mathbb{Z} \times \mathbb{Z}^*$.
Lorsque $\exists k \in \mathbb{Z}$ tel que $a = b.k$, on dira que : b *divise* a (noté $b \ / \ a$ ou $b \mid a$).

Remarque 2.

1. Dire que $b \mid a$ revient à dire que le reste de la division euclicidienne de a par b est nul (en maple : `irem(a,b)=0`).
2. On note $b\mathbb{Z}$ l'ensemble des nombres divisibles par b. Ces nombres sont appelés les *multiples* de b.

$$\boxed{b \text{ divise } a \iff a \text{ multiple de } b}$$

3. La relation "divise" définit une relation d'ordre partielle sur $\mathbb{N}$. En particulier, on a $b \mid a \Rightarrow |b| \leq |a|$.

PROPOSITION 2 : **Propriétés de la divisibilité**
Soient a, b, c, d, λ et μ dans $\mathbb{Z}$.

1. Si $\begin{cases} a/b \\ c/d \end{cases}$ alors ac/bd
2. Si $\begin{cases} a/b \\ b/a \end{cases}$ alors $a = \pm b$
3. Si $\begin{cases} a/b \\ a/c \end{cases}$ alors $a/(\lambda b + \mu c)$
4. Si $\begin{cases} a/b \\ b/c \end{cases}$ alors a/c

Preuve 2 : Aucune difficulté!

Remarque 3. La proposition 2. sera très utilisée pour démontrer des égalités.

Remarque 4. Comme le montre les exemples suivants, les relations de divisibilité permettent de résoudre des équations d'entiers.

`Exemple` 2. (∗) Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $x - 1 \mid x + 3$
2. $xy = 2x + 3y$

`Exemple` 3. (∗)
1. Montrer que pour tout $n \in \mathbb{N}$, $3^{2n} - 2^n$ est un multiple de 7.
2. Montrer que $11 \mid 2^{123} + 3^{121}$.
3. Montrer que pour tout $n \in \mathbb{N}$: $6 \mid 5n^3 + n$

2 Les congruences

DÉFINITION 2 : **La notation "congruence"**
Soient trois entiers a, b et c.
Lorsqu'il existe $k \in \mathbb{Z}$ tels que $a = b + kc$, on écrit : $\boxed{a \equiv b\ [c]}$
On dit que "a est congru à b modulo c"

Remarque 5. Ainsi, si r est le reste de la division euclidienne de a par b, on a : $a \equiv r\ [b]$

PROPOSITION 3 : **Opérations sur les congruences**
Les nombres intervenant dans les propriétés suivantes sont tous des entiers.

P_1 Si $\begin{cases} a_1 \equiv b_1\ [n] \\ a_2 \equiv b_2\ [n] \end{cases}$ alors : $a_1.a_2 \equiv b_1.b_2\ [n]$ et $a_1 + a_2 \equiv b_1 + b_2\ [n]$.

P_2 Si $a \equiv b\ [n]$ alors :
- pour tout $p \in \mathbb{N}$ on a : $a^p \equiv b^p\ [n]$
- pour tout $k \in \mathbb{Z}$, on a : $\begin{cases} k.a \equiv k.b\ [n] \\ k.a \equiv k.b\ [kn] \end{cases}$ et $k + a \equiv k + b\ [n]$
- $b \equiv a\ [n]$
- $a - b \equiv 0\ [n]$

P_3 Si $\begin{cases} a \equiv b\ [n] \\ b \equiv c\ [n] \end{cases}$ alors : $a \equiv c\ [n]$ (transitivité)

Preuve 3 : Pas de difficulté ...

Remarque 6. On a aussi l'équivalence suivante : b divise $a \iff a \equiv 0\ [b]$

`Exemple` 4. (∗) Soit $n \in \mathbb{Z}$. Montrer que $\begin{cases} n^1 \equiv 0\ [4] \text{ ou } n^2 \equiv 4\ [8] & \text{si } n \text{ est pair} \\ n^2 \equiv 1\ [8] & \text{si } n \text{ est impair} \end{cases}$

Exercice : 1
(∗∗) Soient $a \in \mathbb{Z}$ impair et $n \in \mathbb{N}$ tel que $n \geq 3$.
Montrer que $a^{2^{n-2}} \equiv 1\ [2^n]$.

Définition 3 : **L'anneau $\mathbb{Z}/n\mathbb{Z}$**
Soit $n \in \mathbb{N}^*$ tel que $n \geq 2$.
L'ensemble $\{0, 1, \ldots, n-1\}$ est noté $\mathbb{Z}/n\mathbb{Z}$ lorsqu'il est muni des lci $+$ et $\times$ définies de la façon suivante :

1. $a + b =$ le reste de la division euclidienne de $a + b$ par n.
2. $a \times b =$ le reste de la division euclidienne de $a \times b$ par n.

On montre alors que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

3 PGCD et PPCM

Définition 4 : **PGCD et PPCM**
Soient a et b deux entiers relatifs non nuls.

1. L'ensemble des entiers de $\mathbb{N}^*$ diviseurs communs à a et b admet un plus grand élément δ noté $\delta = a \wedge b$. C'est le *plus grand commun diviseur* des entiers a et b.
2. L'ensemble des entiers de $\mathbb{N}^*$ multiples communs de a et b admet un plus petit élément μ noté $\mu = a \vee b$. C'est le *plus petit commun multiple* des entiers a et b.

Exercice : 2
(**) Cet exercice permet de mettre en évidence des propriétés importantes du PGCD.
Il pourra être utile de retenir les méthodes mises en oeuvre ...

1. Soient H_1 et H_2 deux sous-groupes de $(\mathbb{Z}, +)$.
   On définit l'ensemble $H_1 + H_2 = \{h_1 + h_2 \mid (h_1, h_2) \in H_1 \times H_2\}$.
   Montrer que $H_1 + H_2$ est le plus petit (au sens de l'inclusion) sous-groupe de $(\mathbb{Z}, +)$ qui contient la partie $H_1 \cup H_2$.

2. Application du résultat précédent :
   Soient a et b deux entiers naturels non nuls.
   (a) Justifier que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$ avec $\delta \in \mathbb{N}^*$ un diviseur commun à a et b.
   (b) Soit d un diviseur commun à a et b.
      i. Montrer que $a\mathbb{Z} \cup b\mathbb{Z} \subset d\mathbb{Z}$.
      ii. En déduire que δ est le PGCD de a et b.
   (c) Bilan : Citer 2 propriétés importantes liées au PGCD de deux entiers.
   (d) Déduire des deux questions précédentes le sous-groupe $4\mathbb{Z} + 6\mathbb{Z}$.

Remarque 7.

1. Le PPCM de deux entiers permet de limiter les calculs lors de l'addition de deux fractions rationnelles.
2. Le PGCD de deux entiers permet de transformer une fraction rationnelle en une fraction irréductible.
3. Dans la recherche du PGCD ou du PPCM on pourra, si on le souhaite, changer un des nombres en son opposé.
4. les lois $\wedge$ et $\vee$ sont commutatives.

3.1 L'algorithme d'Euclide et ses conséquences

Théorème Fondamental 4 : **Théorème d'Euclide**
Pour tout entiers relatifs a et b non nuls.
Si $a = bq + r$ est la division euclidienne de a par b, alors : $PGCD(a, b) = PGCD(b, r)$.

Preuve 4 : On montre sans difficulté que $\{a, b\}$ et $\{b, r\}$ ont même ensemble de diviseurs communs.

Pour prouver l'égalité de deux PGCD ($a \wedge b = e \wedge f$), on pourra prouver que les deux couples (a, b) et (e, f) ont même ensemble de diviseurs commun. Cela revient à raisonner de la façon suivante :

1. Soit d un diviseur commun à a et b, montrons que $\begin{cases} d \mid e \\ d \mid f \end{cases}$ ...
2. Soit d un diviseur commun à e et f, montrons que $\begin{cases} d \mid a \\ d \mid b \end{cases}$ ...

Algorithme d'Euclide
Le théorème précédent permet de construire un algorithme permettant de déterminer le PGCD de deux entiers non nuls a et b.

1. On pose $r_0 = a$ et $r_1 = b$
2. On construit alors une suite (r_k) strictement décroissante de *restes* en effectuant, tant que $r_k \neq 0$, la division euclidienne de r_{k-1} par r_k et en appelant r_{k+1} le nouveau reste obtenu.
$$r_{k-1} = r_k.q_k + r_{k+1}$$
3. D'après le théorème d'Euclide, on a $r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$.
Comme (r_k) est une suite d'entiers strictement décroissante, il existe un rang n tel que $r_n \neq 0$ et $r_{n+1} = 0$.
4. On a alors $\left\{ \begin{array}{l} a \wedge b = r_n \wedge r_{n-1} \\ r_n / r_{n-1} \end{array} \right.$ et ainsi : $\boxed{r_n = a \wedge b}$

`Exemple` 5. $(*)$ Utiliser l'algorithme d'Euclide pour déterminer le PGCD de $a = 2004$ et $b = 835$.

Dessin

Algorithme d'Euclide

Exercice : 3
$(*)$ Construire en langage Maple une procédure mettant en oeuvre l'algorithme d'Euclide.

1. Avec une boucle `while` (un peu technique)
2. Sous une forme récursive. (facile)

COROLLAIRE 5 : **Caractérisation des diviseurs et multiples communs à a et b**

Soient deux entiers a et b.
1. d est un diviseur commun de a et b ssi d divise $a \wedge b$
2. m est un multiple commun de a et b ssi m est un multiple de $a \vee b$

Preuve 5 :

1. $\Rightarrow$ C'est une conséquence de l'algorithme précédent. (ou de l'exercice précédent !)
   $\Leftarrow$ Evident !
2. $\Rightarrow$ On considère m un multiple de a et b.
   Pour prouver que m est un multiple de $\mu = a \vee b$, on peut effectuer la division euclidienne de m par μ et on montre que le reste est nécessairement nul.
   $\Leftarrow$ Evident !

Remarque 8. Ainsi, si a et b divise un entier c alors $a \vee b$ divise aussi c.

COROLLAIRE 6 : **Le PGCD et le PPCM sont associatifs**

Pour tout entiers relatifs a, b et c non nuls, on a : $\left\{ \begin{array}{l} (a \wedge b) \wedge c = a \wedge (b \wedge c) \\ (a \vee b) \vee c = a \vee (b \vee c) \end{array} \right.$

Preuve 6 :

1. On prouve que $\left\{ \begin{array}{l} a \wedge b \\ c \end{array} \right.$ et $\left\{ \begin{array}{l} a \\ b \wedge c \end{array} \right.$ ont même ensemble de diviseurs communs.
2. Même idée pour l'associativité de $\vee$.

Remarque 9. On peut ainsi définir le PGCD et le PPCM de n entiers : $\left\{ \begin{array}{l} \text{pgcd}(x_1, \ldots, x_n) = x_1 \wedge \cdots \wedge x_n \\ \text{ppcm}(x_1, \ldots, x_n) = x_1 \vee \cdots \vee x_n \end{array} \right.$

`Exemple` 6. $(*)$ Déterminer le PGCD des nombres suivants : 34, 56, 45, 124.

3.2 Le théorème de Bezout

THÉORÈME FONDAMENTAL 7 : **Théorème de Bezout**
Soient a et b deux entiers relatifs non nuls.
On a :

$$\delta = a \wedge b \quad \Rightarrow \quad \exists (u, v) \in \mathbb{Z}^2 \quad \text{tels que} \quad au + bv = \delta$$

Preuve 7 : La démonstration est donnée par l'algorithme suivant. (ou par un exercice traité précédemment !)

Remarque 10.

1. On dira que (u, v) tel que $au + bv = \delta$ est un *couple de Bezout* associé à a et b.
2. On retrouve ainsi le fait qu'un diviseur commun à a et b divise aussi $a \wedge b$.
3. Comme on le verra plus tard, il existe une infinité de couples de Bezout.
4. ⚠ : la réciproque de ce théorème n'est vraie que si δ est un diviseur commun à a et b.
5. Le théorème de Bezout est très souvent utilisé dans les exercices ou les démonstrations.

Algorithme pour trouver un couple de Bezout
Soient a et b deux entiers relatifs non nuls tels que $a \wedge b = \delta$.
On pourra trouver un couple de Bezout associé à a et b en procédant de la façon suivante :

1. On applique l'algorithme d'Euclide à a et b.
   On construit ainsi les suites (r_k) et (q_k) telles que $r_{k-1} = q_k.r_k + r_{k+1}$ avec $0 < r_{k+1} < r_k$.
   Notons $r_n = \delta$ le dernier terme non nul de la suite (r_k).
2. On définit simultanément les suites (u_k) et (v_k) telles que $r_k = u_k a + v_k b$ pour tout $k \in [\![1,n]\!]$.
   On a alors $\begin{cases} (u_0, v_0) = (1, 0) \\ (u_1, v_1) = (0, 1) \end{cases}$ et $\begin{cases} u_{k+1} = u_{k-1} - q_k u_k \\ v_{k+1} = v_{k-1} - q_k v_k \end{cases}$
3. Comme d'autre part $\delta = u_n a + v_n b$, alors les coefficients de Bezout sont u_n et v_n.
4. On pourra présenter les calculs intermédiaires dans un tableau de la forme :

$r_0 = a$	$r_1 = b$	r_2	$\dots$	r_k	$\dots$	δ
	q_1	q_2	$\dots$	q_k	$\dots$	
1	0	u_2	$\dots$	u_k	$\dots$	$u_n = u$
0	1	v_2	$\dots$	v_k	$\dots$	$v_n = v$

`Exemple` 7. (∗) Appliquer l'algorithme précédent pour déterminer :

1. un couple de Bezout pour $a = 22$ et $b = 17$.
2. un couple de bezout pour $a = 127$ et $b = 35$.

`Exemple` 8. (∗∗) Sauriez-vous construire un programme déterminant un couple de Bezout pour un couple (a, b) donné ?

4 Les nombres premiers entre eux

DÉFINITION 5 : **Nombres premiers entre eux**
Soient a et b deux entiers relatifs non nuls.
On dit que a et b sont *premiers entre eux* ssi $a \wedge b = 1$

`Exemple` 9. (∗) Démontrer que deux entiers naturels consécutifs sont premiers entre eux.

Remarque 11. On dira qu'une fraction a/b est *irréductible* ssi $a \wedge b = 1$.

Exercice : 4
(∗) Prouver que la fraction $\dfrac{21n + 4}{14n + 3}$ est irréductible pour tout $n \in \mathbb{N}$.

Remarque 12. On peut bien entendu étendre cette définition à n nombres entiers non nuls :

$$a_1, \dots, a_n \text{ sont premiers entre eux} \quad \Longleftrightarrow \quad a_1 \wedge \dots \wedge a_n = 1.$$

1. ⚠ n entiers peuvent être premiers entre eux sans être premiers entre eux deux à deux.
   Montrer que les entiers 10, 6 et 15 sont premiers entre eux. Le sont-ils deux à deux ?
2. Prouver que si parmi n entiers, deux sont premiers entre eux, alors ils sont premiers entre eux.

THÉORÈME FONDAMENTAL 8 : **Théorème de Bezout (bis)**
Soient a et b deux entiers relatifs non nuls.
On a :
$$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2 \text{ tels que } au + bv = 1$$

Preuve 8 :
$\Rightarrow$ Conséquence immédiate du théorème de Bezout.
$\Leftarrow$ Comme $a \wedge b$ divise a et b, alors il divise $au + bv$, c'est à dire 1.

`Exemple` 10. $(*)$ Soit $n \in \mathbb{N}^*$ avec $n \geq 2$. Déterminer les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$.
Dans quel cas $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est-il un corps?

COROLLAIRE 9 :
Si a, b et c sont 3 entiers relatifs non nuls alors : $\begin{cases} c \text{ divise } a \\ a \wedge b = 1 \end{cases} \Rightarrow c \wedge b = 1.$

Preuve 9 :
M1 : On utilise l'égalité de Bezout pour traduire $a \wedge b = 1$.
M2 : On peut aussi effectuer une démonstration directe.

COROLLAIRE 10 : **Caractérisation du PGCD**
Si a et b sont 2 entiers relatifs non nuls, vérifiant $\begin{cases} a = a'\delta \\ b = b'\delta \end{cases}$ alors : $\boxed{\delta = a \wedge b \iff a' \wedge b' = 1}$.

Preuve 10 :
M1 : Immédiat avec le théorème de Bezout.
M2 : On peut aussi prouver ce résultat par double contraposée.

Remarque 13. Cette propriété est souvent utilisée en arithmétique.

COROLLAIRE 11 :
- Si a, b et c sont 3 entiers relatifs non nuls, alors : $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Rightarrow a \wedge bc = 1.$
- De façon plus générale :
  1. si a est premier avec $b_1, \ldots$ et b_k alors $a \wedge b_1 \ldots b_k = 1$.
  2. si a est premier avec b alors $a^p \wedge b^q = 1$ pour tout $(p, q) \in \mathbb{N}^{*2}$

Preuve 11 : Immédiat avec le théorème de Bezout, puis on généralise par récurrence.

`Exemple` 11. $(*)$ Si a et b sont premiers entre eux, montrer que $ab \wedge (a + b) = 1$.

PROPOSITION 12 : **Relation entre PGCD et PPCM**
Soient a et b deux entiers relatifs non nuls.
$$\boxed{(a \wedge b)(a \vee b) = |ab|}$$

Preuve 12 :
1. On pose $\begin{cases} \delta = a \wedge b \\ \mu = a \vee b \end{cases}$ et $\begin{cases} a = \delta.a' \\ b = \delta.b' \end{cases}$.
2. Remarquons que $\delta.a'.b'$ est un multiple commun à a et b et donc à μ, donc : $\exists k \in \mathbb{N}$ tel que $\delta.a'.b' = k.\mu$
3. Comme μ est un multiple commun à a et b, on a d'autre part : $\begin{cases} \mu = \alpha.a \\ \mu = \beta.b \end{cases}$. Ainsi : $\begin{cases} b' = k\alpha \\ a' = k\beta \end{cases}$.
4. Or, comme $a' \wedge b' = 1$ alors $k = \pm 1$. Et donc : $\delta.|a'.b'| = \mu$.
5. On conclut en multipliant par δ.

Remarque 14. Ainsi :
1. si $a \wedge b = 1$ alors $\boxed{a \vee b = |ab|}$
2. si $\begin{cases} a = a'\delta \\ b = b'\delta \end{cases}$ avec $a' \wedge b' = 1$ alors $\boxed{a \vee b = |\delta a' b'|}$

`Exemple` 12. (∗) Déterminer le PGCD et le PPCM de $a = 2004$ et $b = 835$.

`Exemple` 13. (∗) Résoudre dans $\mathbb{N}^2$ le système $\begin{cases} x \wedge y = 5 \\ x \vee y = 60 \end{cases}$.

PROPOSITION 13 : Si a, b et c sont 3 entiers relatifs non nuls alors : $\begin{cases} 1. & (ca) \wedge (cb) = |c|(a \wedge b) \\ 2. & (ca) \vee (cb) = |c|(a \vee b) \end{cases}$

Preuve 13 :
1. On écrit que $\begin{cases} a = \delta a' \\ b = \delta b' \end{cases}$ avec $a' \wedge b' = 1$. On a alors $\begin{cases} ac = c\delta a' \\ bc = c\delta b' \end{cases}$ avec $a' \wedge b' = 1$... cqfd ...
2. On déduit 2. de 1. à l'aide de $|ab| = (a \wedge b)(a \vee b)$.

COROLLAIRE 14 : Si a et b sont deux entiers relatifs non nuls alors : $a^k \wedge b^k = (a \wedge b)^k$ pour tout $k \in \mathbb{N}^*$

Preuve 14 : On note $\delta = a \wedge b$ et $d = a^k \wedge b^k$ et on montre que $d = \delta^k$.
Pour cela, on calcule $d = a^k \wedge b^k = ...$ en exprimant $\begin{cases} a = a'.\delta \\ b = b'.\delta \end{cases}$ avec $a' \wedge b' = 1$.

`Exemple` 14. (∗) Prouver que si $x \wedge y \wedge z = 1$ alors $x^2 \wedge y^2 \wedge z^2 = 1$

Exercice : 5
(∗) Soit a et b deux entiers relatifs tels que a^2/b^2. Montrer que a/b.

THÉORÈME FONDAMENTAL 15 : **Théorème de Gauss**
Soient a, b et c trois entiers relatifs non nuls.
On a :

$$\text{Si} \quad \begin{cases} a \text{ divise } bc \\ a \wedge b = 1 \end{cases} \quad \text{alors} \quad a \text{ divise } c$$

Preuve 15 : Conséquence immédiate du théorème de Bezout.

Exercice : 6
(∗∗) Soient a et b deux entiers non nuls premiers entre eux et un couple de Bezout $(u_0, v_0) \in \mathbb{Z}^2$ tel que $au_0 + bv_0 = 1$.
1. Déterminer tous les couples d'entiers $(u, v) \in \mathbb{Z}^2$ tels que : $au + bv = 1$.
2. Si a, $b \in \mathbb{N}^*$, montrer qu'il existe deux entiers $(u, v) \in \mathbb{Z}^2$ tels que : $au + bv = 1$ et $\begin{cases} |u| < b \\ |v| \leq a \end{cases}$

Exercice : 7
Equations diophantiennes
(∗) Soient A, B et C trois entiers relatifs non nuls et on considère l'équation :

$$(E) \ : \ Ax + By = C \quad \text{avec } (x, y) \in \mathbb{Z}^2$$

Le but de cet exercice est de déterminer une méthode permettant de résoudre cette équation.
1. Soit $\delta = A \wedge b$. Montrer que si δ ne divise pas C alors $\mathcal{S} = \emptyset$.
   En divisant par δ, l'équation (E) se ramène donc à (E') : $A'x + B'y = C'$ avec $A' \wedge B' = 1$.
2. Comment trouver une solution particulière de (E') ?
3. En déduire l'ensemble $\mathcal{S}$ de toutes les solutions.
4. Résoudre dans $\mathbb{Z}$ les équations : $13x + 5y = 4$ et $24x + 20y = 36$

COROLLAIRE 16 : Soient a, b et c trois entiers relatifs non nuls. $\begin{cases} a \text{ divise } c \\ b \text{ divise } c \\ a \wedge b = 1 \end{cases} \Rightarrow ab$ divise c

Preuve 16 : Immédiat avec le théorème de Gauss.

Remarque 15. La relation précédente se généralise au cas a est divisible par $b_1, \ldots, b_k$ avec les b_i premiers entre eux deux à deux.

`Exemple` 15. (∗) Soit $p > 3$ un nombre premier. Montrer que $24 \mid p^2 - 1$.

5 Les nombres premiers

DÉFINITION 6 : **Nombre premier**
Dans $\mathbb{N}^*$, on dira qu'un nombre est premier ssi : $\begin{cases} \text{il est différent de 1} \\ \text{il n'admet pas d'autre diviseur que 1 et lui-même} \end{cases}$.
On pourra noter $\mathcal{P}$ l'ensemble des nombres premiers.

Remarque 16. Les nombres premiers sont les *atomes* de l'arithmétique. Comme les atomes permettent en chimie de construire toutes les molécules, nous verrons en effet que les nombres premiers engendrent l'ensemble des nombres entiers.

Remarque 17. Le crible d'érathostène permet de déterminer les premiers nombres premiers.

Exercice : 8
(∗∗) Soit a et p deux entiers supérieurs à 2. Montrer que si $a^p - 1$ est premier alors $\begin{cases} a = 2 \\ p \text{ est premier} \end{cases}$

Pour prouver qu'un nombre n'est pas premier, on pourra montrer que :
1. il s'écrit sous la forme $n = ab$ avec $a, b \in \mathbb{Z}$
2. que $\begin{cases} a \geq 2 \\ b \geq 2 \end{cases}$

Remarque 18. Un nombre entier qui n'est pas premier est dit *composé*.

`Exemple` 16. (∗∗) Montrer que $\forall n \in \mathbb{N}^*$, $4n^3 + 6n^2 + 4n + 1$ est un nombre composé.

5.1 Propriétés des nombres premiers

PROPOSITION 17 : **Propriétés des nombres premiers**
1. Soit $p \in \mathbb{N}$ un nombre premier et $n \in \mathbb{Z}$. Alors, soit p divise n, soit $p \wedge n = 1$.
2. Deux nombres premiers distincts sont premiers entre eux.
3. Si un nombre premier divise un produit d'entiers, alors il divise l'un d'entre eux.

Preuve 17 :
1. Pas de difficulté.
2. Pas de difficulté.
3. On applique le théorème de Gauss et la propriété 1.

Remarque 19. Ainsi, si un nombre premier p divise m^k alors p divise m.

`Exemple` 17. (∗∗) Soit p un nombre premier. Prouver que $\sqrt{p}$ est un irrationnel.

THÉORÈME 18 : Tout entier naturel $n \geq 2$ admet un diviseur premier.

Preuve 18 :
1. Méthode 1 : Par récurrence (forte) ...
2. Méthode 2 : On note $\mathcal{D}(n)$ l'ensemble des entiers naturels différents de 1 qui divisent n.
   $\mathcal{D}(n)$ est une partie de $\mathbb{N}$ non vide, donc il admet un plus petit élément.
   On montre alors que cet élément est un nombre premier.

THÉORÈME 19 :
Tout entier composé n admet un diviseur premier $p \leq \sqrt{n}$.

Preuve 19 : On note $n = ab$ avec $\begin{cases} a \geq 2 \\ b \geq 2 \end{cases}$. On montre que $\begin{cases} a > \sqrt{n} \\ b > \sqrt{n} \end{cases}$ est impossible...
Puis, on suppose par exemple que $a \leq \sqrt{n}$ et comme a admet un diviseur premier ...

Remarque 20. Ainsi, un entier n qui n'admet pas de diviseur premier inférieur à $\sqrt{n}$ est un nombre premier.
Cette remarque permet de limiter les calculs dans la recherche de nombres premiers par le crible d'érathostène.

`Exemple` 18. (∗) Prouver que 167 est un nombre premier.

Exercice : 9

(∗∗) Soit m un entier strictement plus grand que 1.
Montrer que si m divise $(m-1)!+1$ alors m est premier.

THÉORÈME FONDAMENTAL 20 : **Infinité des nombres premiers**
Il existe une infinité de nombres premiers.

Preuve 20 : Il existe un grand nombre de démonstrations possibles.
Procédons ici par l'absurde en supposant que $\mathcal{P} = \{p_1, \ldots, p_k\}$.
On considère alors l'entier $a = p_1.p_2 \ldots p_k + 1$.
Comme a est un nombre composé (puisque strictement supérieur à tous les p_i), il est divisible par l'un des p_i.
Et comme a et $p_1.p_2 \ldots p_k$ sont divisibles par ce p_i alors 1 l'est aussi ... ce qui est impossible !

5.2 Décomposition d'un entier en produit de facteurs premiers

THÉORÈME FONDAMENTAL 21 : **Décomposition d'un entier en produit de facteurs premiers**
Tout entier naturel $\begin{cases} n \in \mathbb{N} \\ n \geq 2 \end{cases}$ se décompose de façon unique en produit de facteurs premiers.

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p}$$

où :
1. $\mathcal{P}$ est l'ensemble des nombres premiers
2. $(\alpha_p)_{p \in \mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$
3. $v_p(n) = \alpha_p$ est appelée la *p-valuation* de l'entier n.

Preuve 21 : On peut démontrer l'existence par une récurrence forte et l'unicité de façon classique.

Remarque 21. Pour deux entiers naturels non nuls a et b, on a : $v_p(a \times b) = v_p(a) + v_p(b)$

Exercice : 10

(∗∗) Soient x, y et z trois entiers et X, Y et Z les ensembles de nombres premiers intervenant dans leurs décompositions en facteurs premiers respectives.
1. Montrer que : $x \wedge y \wedge z = 1 \iff X \cap Y \cap Z = \emptyset$.
2. En déduire que : $x \wedge y \wedge z = 1 \iff x^2 \wedge y^2 \wedge z^2 = 1$

PROPOSITION 22 : **Diviseurs d'un entier naturel**
Soit $n \in \mathbb{N}^*$ de décomposition en facteurs premiers : $n = \prod_{p \in \mathcal{P}} p^{n_p}$.
Les diviseurs de n sont les entiers

$$d = \prod_{p \in \mathcal{P}} p^{d_p} \quad \text{avec} \quad \forall p \in \mathcal{P},\ 0 \leq d_p \leq p$$

Preuve 22 : On considère $d = \prod_{p \in \mathcal{P}} p^{d_p}$ et on montre à quelles conditions ce nombre divise n.

`Exemple` 19. (∗) La décomposition en facteurs premiers reste un problème très difficile pour les grands nombres. En revanche, elle ne pose pas de difficulté pour les *petits* nombres.
1. Décomposer 2004 en facteurs premiers.
2. Déterminer l'ensemble de ses diviseurs

Exercice : 11

(∗∗) Résoudre dans $\mathbb{N}^2$ l'équation $11(a \wedge b) + (a \vee b) = 203$ avec $a \leq b$.

Exercice : 12

(∗∗) Soit $n \in \mathbb{N}\backslash\{0;1\}$ dont la décomposition en nombre premier est $n = \prod_{i=1}^{N} p_i^{\alpha_i}$.
On note $d(n)$ le nombre de diviseurs supérieurs ou égaux à 1 de n et $\sigma(n)$ la somme de ceux-ci.
Montrer que :

1. $d(n) = \prod_{i=1}^{N}(\alpha_1 + 1)$

2. $\sigma(n) = \prod_{i=1}^{N} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$

COROLLAIRE 23 : **Expression du PGCD et du PPCM**
Soient a et b deux entiers naturels non nuls de décompositions en facteurs premiers suivantes :

$$a = \prod_{p\in\mathcal{P}} p^{v_p(a)} \quad \text{et} \quad b = \prod_{p\in\mathcal{P}} p^{v_p(b)}$$

On a alors :

$$\boxed{a \wedge b = \prod_{p\in\mathcal{P}} p^{\min(v_p(a),\ v_p(b))}} \quad \text{et} \quad \boxed{a \vee b = \prod_{p\in\mathcal{P}} p^{\max(v_p(a),\ v_p(b))}}$$

Preuve 23 :
1. Tous les diviseurs communs à a et b divisent $\prod_{p\in\mathcal{P}} p^{\min(v_p(a),\ v_p(b))}$ qui divise aussi a et b.
2. Il suffit d'utiliser la relation $(a \wedge b)(a \vee b) = ab$.

Remarque 22. a et b sont donc premiers entre eux si et seulement si, ils n'ont pas de nombre premier en commun dans leur décomposition en facteur premier.

`Exemple` 20. $(*)$ Déterminer le PGCD et le PPCM de $a = 6513$ et $b = 2004$.

Exercice : 13
$(*)$ Refaire l'exemple 6 et l'exemple 13 en utilisant ce théorème.

COROLLAIRE 24 :
Les lois $\wedge$ et $\vee$ sont distributives l'une sur l'autre : $\begin{cases} a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \end{cases}$

Preuve 24 : Démonstration admise. Elle utilise les formules démontrées dans le corollaire précédent.