**Filière** : **SMIA** 1

# Arithmétique des Entiers

**Abdallah Hammam**
**Université Moulay Ismaïl**
**Faculté des sciences**
**Département de Mathématiques**
**Meknès - Morocco.**

a.hammam@fs.umi.ac.ma

Toute remarque venant de votre part sera la bienvenue.

Si vous trouvez une erreur, merci de la signaler.

vous aurez un POINT de plus à l'examen.

# Table des matières


**1 Arithmétique des entiers** **5**

1.1 Construction de l'ensemble $\mathbb{N}$ des Entiers Naturels : Axiomes de Péano . . . 5

1.2 Addition et multiplication dans l'ensemble $\mathbb{N}$ . . . 7

1.2.1 Addition de deux entiers . . . 7

1.2.2 Multiplication de deux entiers . . . 7

1.3 Propriétés de l'Addition et de la multiplication . . . 7

1.3.1 Commutativité . . . 7

1.3.2 Associativité . . . 8

1.3.3 Distributivité de la multiplication par rapport à l'addition . . . 8

1.3.4 Construction de l'ensemble $\mathbb{Z}$ des Entiers Relatifs . . . 8

1.4 Division Euclidienne, diviseur et multiple . . . 9

1.4.1 Division Euclidienne dans $\mathbb{N}$ . . . 9

1.4.2 Diviseur et Multiple dans $\mathbb{N}$ . . . 10

1.4.3 Notion de Diviseur Commun . . . 11

1.4.4 Plus Grand Commun Diviseur : pgcd . . . 12

1.4.5 Plus Petit Commun Multiple : ppcm . . . 13

1.4.6 Lemme d'Euclide : Base des autres théorèmes . . . 13

1.4.7 Algorithme d'Euclide . . . 14

1.5 Théorème de Bezout et ses Corollaires . . . 15

1.5.1 Algorithme d'Euclide étendu et Identité de Bezout . . . 15

1.5.2 Théorème de Bezout . . . 17

1.5.3 Résolution des équations Diophantiennes . . . 19

1.5.4 Théorème de Gauss . . . 20

1.6 La Notion de Congruence . . . 21

1.6.1 Définition . . . 22

1.6.2 Compatibilité de la congruence avec l'addition . . . 24

1.6.3 Compatibilité de la congruence avec la multiplication . . . 24

1.6.4 Compatibilité de la congruence avec la puissance . . . 24

1.6.5 L'anneau quotient $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ . . . 25

**2 Notion de Primalité dans $\mathbb{N}$** **27**

2.1 Nombres Premiers . . . 27

2.1.1 Y a-t-il une infinité de Nombres Premiers ?? . . . 28

2.1.2 Théorème fondamental de l'arithmétique . . . 30

2.1.3 Un test de primalité : Le Théorème de Wilson . . . 32

2.1.4 Lien entre nombres premiers et Fonction " Dzéta ($\zeta$) " de Riemann . 34
2.2 Indicateur ou Fonction indicatrice d'Euler et application à la cryptographie . 34
2.2.1 Propriétés de la fonction indicatrice . . . . . 35
2.2.2 Théorème d'Euler . . . . . 38
2.2.3 Théorème de Fermat . . . . . 40
2.2.4 Le Logarithme discret . . . . . 40
2.2.5 L'algorithme de cryptage RSA . . . . . 40
2.2.6 Comment ça marche ? . . . . . 41
2.2.7 Pourquoi ça marche ? . . . . . 41

# Chapitre 1

# Arithmétique des entiers

## 1.1 Construction de l'ensemble $\mathbb{N}$ des Entiers Naturels : Axiomes de Péano

Dieu a créé les entiers pour les enfants et l'adulte a fait le reste, et pas que.

L'arithmétique de Péano permet de Construire ou de définir l'ensemble $\mathbb{N}$ des entiers naturels, à partir des 5 axiomes suivants :

Axiome 1 : L'ensemble $\mathbb{N}$ est non vide
0 est un entier naturel.

Axiome 2 : Existence d'une application $S$ de $\mathbb{N}$ vers $\mathbb{N}$
Tout entier naturel $n$ admet un successeur, noté $S(n)$ qui est lui même un entier naturel.
De ce fait, $S(0), S(S(0)), S(S(S(0))), ...$ sont des entiers naturels.

Axiome 3 : Le plus petit élément de $\mathbb{N}$
Il n'existe aucun entier naturel dont le successeur serait $0 : \mathbb{N}$ est bien ordonné $(\leq .)$

$$(\forall n \in \mathbb{N}) \quad S(n) \neq 0$$

Axiome 4 : Injectivité de l'application $S$
Deux entiers naturels qui ont le même successeur sont égaux.

$$(\forall (n, m) \in \mathbb{N}^2) \quad \Big(S(n) = S(m) \quad \Longrightarrow \quad n = m\Big)$$

Axiome 5 : Principe de la récurrence
Si $E$ est un ensemble tel que

1. $$0 \in E$$
2. $$(\forall n \in E) \;\; S(n) \in E$$

$$\text{Alors, } \ E = \mathbb{N}.$$

Cet axiome constitue la base du raisonnement par récurrence . En effet, si $P(n)$ est un prédicat de domaine $\mathbb{N}$, Alors pour montrer que

$$(\forall n \in \mathbb{N}) \ \ P(n)$$

Il suffit de poser $E = \{n \in \mathbb{N} \ \ : \ \ P(n)\}$, puis de montrer que

1.
$$0 \in E$$

2.
$$(\forall n \in E) \quad n+1 \in E$$

C'est à dire

1.
$$P(0)$$

2.
$$(\forall n \in \mathbb{N}) \quad \Big(P(n) \implies P(n+1)\Big)$$

et de conclure, grâce à cet axiome que $E = \mathbb{N}$ ou en d'autres termes

$$(\forall n \in \mathbb{N}) \quad P(n)$$

**remarque 1.** *Ces axiomes permettent alors de poser, par construction, que*

$$\begin{aligned}\mathbb{N} &= \{0, S(0), S(S(0)), S(S(S(0))), ...\} \\ &= \{\nabla, \diamondsuit, \triangle, \clubsuit, ...\} \\ &= \{0, 1, 2, 3, ...\}\end{aligned}$$

*et*

$$\mathbb{N}^* = \{1, 2, 3, ...\} = \ \textit{l'ensemble des entiers naturels non nuls.}$$

*De plus, Ces axiomes offrent les conclusions suivantes* <u>*à retenir*</u> *:*

1. *Tout partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*

2. *Toute partie non vide majorée de* $\mathbb{N}$ *admet un plus grand élément.*

3. *Toute partie non vide finie de* $\mathbb{N}$ *admet un plus petit et un plus grand élément.*

## 1.2 Addition et multiplication dans l'ensemble $\mathbb{N}$

Maintenant que Notre ensemble $\mathbb{N}$ des entiers naturels est bien construit, nous pouvons définir

des lois de composition internes (addition (+), multiplication ($\times$ ou .)),

des relations d'équivalences (égalité (=), congruence ($\equiv$)),

des relations d'ordre ( comparaison naturelle ($\leq$) , divisibilité (|)),

des prédicats puis des propositions pour enfin énoncer des théorèmes :

Bezout, Gauss, Euler, Fermat et Wilson.
L'idéal, serait de trouver des applications pratiques voire technologiques de ces théorèmes !!

### 1.2.1 Addition de deux entiers

Dans $\mathbb{N}$, La loi de composition interne appelée "addition " et notée +,
est bien définie par les formules suivantes :

$$(\forall n \in \mathbb{N}) \quad n + 0 = n(\ \ 0 \ \text{ est l'élément neutre } )$$

et

$$(\forall (n, m) \in \mathbb{N}^2) \quad n + S(m) = S(n + m)$$

En particulier,

$$(\forall n \in \mathbb{N}) \quad n + S(0) = S(n) = n + 1$$

### 1.2.2 Multiplication de deux entiers

Dans $\mathbb{N}$, La loi de composition interne appelée "multiplication " et notée $\times$,
est bien définie par les deux règles suivantes :

$$(\forall n \in \mathbb{N}) \quad n \times 0 = 0$$

et

$$(\forall (n, m) \in \mathbb{N}^2) \quad n \times S(m) = n \times m + n$$

## 1.3 Propriétés de l'Addition et de la multiplication

### 1.3.1 Commutativité

L'addition et la multiplication dans $\mathbb{N}$ sont commutatives :

$$(\forall (n, m) \in \mathbb{N}^2) \quad n + m = m + n \text{ et } \quad n \times m = m \times n$$

**remarque 2.** *D'après la définition de la multiplication ci-dessus, nous avons en particulier,*

$$(\forall n \in \mathbb{N}) \quad n \times S(0) = n \times 0 + n$$

*c'est à dire*

$$(\forall n \in \mathbb{N}) \quad n \times 1 = n$$

*Ce qui veut dire que* 1 *est l'élément neutre pour la multiplication.*

### 1.3.2 Associativité

L'addition et la multiplication dans $\mathbb{N}$ sont associatives :

$$(\forall (n, m, p) \in \mathbb{N}^3) \quad (n + m) + p = n + (m + p) = n + m + p$$

$$(\forall (n, m, p) \in \mathbb{N}^3) \quad (n \times m) \times p = n \times (m \times p) = n \times m \times p$$

### 1.3.3 Distributivité de la multiplication par rapport à l'addition

$$(\forall (n, m, p) \in \mathbb{N}^3) \quad n \times (m + p) = n \times m + n \times p$$

L'on peut dire que toute l'arithmétique des entiers, repose sur l'algorithme d'Euclide qui est, à son tour, basé essentiellemnt sur la commutativité , l'associativité , et surtout la distributivité .

### 1.3.4 Construction de l'ensemble $\mathbb{Z}$ des Entiers Relatifs

Afin d'obtenir une structure de groupe, sachant que $(\mathbb{N}, +)$ n'en est pas un, on construit un nouvel ensemble, que l'on note $\mathbb{Z}$, en ajoutant à l'ensemble $\mathbb{N}$, tous les symétriques de ses éléments.

$$\mathbb{Z} = \mathbb{N} \cup \{-n, \ n \in \mathbb{N}\} = \{0, 1, 2, 3, ...\} \cup \{0, -1, -2, -3, ...\} = \mathbb{Z}^+ \cup \mathbb{Z}^-$$

**remarque 3.** *Les éléments de l'ensemble* $\mathbb{N}$ *sont les entiers Naturels.*

*Les éléments de l'ensemble* $\mathbb{Z}$ *sont les entiers Relatifs.*

*Les éléments de l'ensemble* $\mathbb{Q}$ *sont les nombres Rationnels.*

*Les éléments de l'ensemble* $\mathbb{R}$ *sont les nombres Réels.*

*Les éléments de l'ensemble* $\mathbb{R} \setminus \mathbb{Q}$ *sont les nombres Irrationnels.*

*Les éléments de l'ensemble* $\mathbb{C}$ *sont les nombres Complexes.*

## 1.4 Division Euclidienne, diviseur et multiple

### 1.4.1 Division Euclidienne dans $\mathbb{N}$

**Lemme 4.** *Soient $a$ un entier naturel et $b$ un entier naturel non nul $b \neq 0$. Alors*

$$\boxed{(\exists\,!\,(q,r)\ \in \mathbb{N}^2)\ :\ a = bq + r \quad avec\ \ 0 \leq r < b}$$

*$q$ et $r$ désignent respectivement le quotient et le reste de la division Euclidienne de $a$ par $b$.*

*$a$ et $b$ sont respectivement le dividende et le diviseur.*

**Exemple 5.**

$$a = 159,\ \ b = 11,\ \ 159 = 14 \times 11 + 5 = 13 \times 11 + 16 \text{ donc } \quad q = 14 \text{ et } \ r = 5.$$

**démonstration 6.** *Commençons d'abord par prouver l'unicité du couple $(q, r)$.*
*Raisonnons par l'absurde et supposons que*

$$a = bq_1 + r_1 = bq_2 + r_2 \ avec \quad 0 \leq r_1 < b \quad et \quad 0 \leq r_2 < b$$

*Il s'en suit que*

$$b(q_1 - q_2) = r_2 - r_1$$

*Ce qui veut dire que*

$$(r_2 - r_1) \quad est\ un\ multiple\ de \quad b$$

*Or*

$$-b < r_2 - r_1 < b$$

*Donc nécessairement*

$$r_2 - r_1 = 0$$

*et par conséquent,*

$$bq_1 = bq_2 \quad ou\ bien \quad q_1 = q_2 \quad CQFD$$

Pour l'existence du couple $(q, r)$ *, distinguons les trois cas :*

1. $0 \leq a < b$
   *Il suffit de remarquer que*

$$a = 0 \times b\ + a \implies \quad q = 0 \quad et \quad r = a$$

2. $a = b$
   *Dans cette situation, nous avons*

$$a = 1 \times b\ + 0 \implies \quad q = 1 \quad et \quad r = 0$$

*3.* $a > b \geq 1$

*Considérons l'ensemble A défini par*

$$A = \{(n \in \mathbb{N}^*) \ : \ nb > a\}.$$

*A est une partie non vide de* $\mathbb{N}$ *car* $a + 7 \in A$.

*En effet* $b \geq 1 \implies (a+7)b \geq a+7 \implies (a+7)b > a \implies (a+7) \in A$.

*A admet alors un plus petit élément que l'on notera p.*

*On a alors*

$$(p-1)b \leq a < bp \quad \textit{c'est à dire} \quad 0 \leq a-(p-1)b < b$$

*Il suffit alors de poser* $q = (p-1)$ *et* $r = a - bq$.

**remarque 7.** *L'on peut définir une division Euclidienne dans l'ensemble des entiers relatifs* $\mathbb{Z}$*, de la façon suivante :*

*Soit* $a > 0$ *tel que* $a = bq + r$ *avec* $0 \leq r < b$ *, alors*

*Si* $r = 0$ *alors* $-a = -bq$ *( le quotient est* $-q$ *, le résidu est* $0$*)*

*et*

*Si* $0 < r < b$ *alors* $-a = -bq - r = -b(q+1) + b - r$ *avec* $0 < b - r < b$ *( le quotient est* $-q$ *, le résidu est* $b - r$*)*

**Exemple 8.**

$$a = -159, \ \ b = 11, \ \ -159 = -14 \times 11 - 5 = -15 \times 11 + 6 \text{ donc} \quad q = -15 \text{ et } \ r = 6.$$

### 1.4.2 Diviseur et Multiple dans $\mathbb{N}$

**Definition 9.** Soient $a$ et $b$ deux entiers naturels.

On dit que $a$ est un multiple de $b$ ou que $b$ est un diviseur de $a$

$$\iff \quad (\exists q \in \mathbb{N}) \ : \ a = qb$$

Dit autrement, $b$ est un diviseur de $a$ Si le reste de la division Euclidienne de $a$ par $b$ est NUL.

Si $b$ est un diviseur de $a$, on écrira

$$b|a \ \text{ ( un trait vertical)}$$

**Exemple 10.**

$$176 = 16 \times 11 \implies 176 \ \text{ est un multiple de } 16,$$

$$176 = 16 \times 11 \implies 176 \ \text{ est un multiple de } 11,$$

$$176 = 16 \times 11 \implies 176 \ \text{ est divisible par } 16,$$

$$176 = 16 \times 11 \implies 176 \ \text{ est divisible par } 11,$$

$$176 = 16 \times 11 \implies 16 \ \text{ est un diviseur de } 176,$$

$$176 = 16 \times 11 \quad \Longrightarrow \quad 11 \quad \text{est un diviseur de } 176.$$

$$176 = 16 \times 11 \quad \Longrightarrow \quad 16 \quad \text{divise } 176,$$

$$176 = 16 \times 11 \quad \Longrightarrow \quad 11 \quad \text{divise } 176 \quad \Longrightarrow \quad 11 \mid 176.$$

**remarque 11.** *1.* $0$ *est un multiple de tout entier naturel (ou même relatif).*

*2. Tout entier naturel est un diviseur de zéro.*

*3.* $1$ *est un diviseur de tout entier.*

*4.* $0$ *ne divise aucun entier naturel. Sauf peut être* $0$*.*

*5. toute combinaison linéaire de multiples est un multiple :*

*Si* $a$ *et* $b$ *sont des multiples de* $n$ *, alors*
$(\forall(\lambda, \mu) \in \mathbb{N}^2) \;\; \lambda.a + \mu.b$ *est un multiple de* $n$*.*

*6. La divisibilité et la multiplicité sont des relations d'ordre partiel.*

**remarque 12.** – *La relation de divisibilité est réflexive :*

$$(\forall a \in \mathbb{N}) \quad a|a$$

– *La divisibilité dans* $\mathbb{N}$ *est antisymétrique*

$$(\forall(a, b) \in \mathbb{N}^2) \;\; \Big((a|b \wedge b|a) \quad \Longrightarrow \quad a = b\Big)$$

– *La divisibilité dans* $\mathbb{Z}$ *n'est ni symétrique, ni antisymétrique*

$$(\forall(a, b) \in \mathbb{Z}^2) \;\; \Big((a|b \wedge b|a) \quad \not\Rightarrow \quad a = b\Big)$$

*(prendre comme contrexemple* $a = 2$ *et* $b = -2$ *)*

– *La divisibilité est transitive*

$$(\forall(a, b, c) \in \mathbb{N}^3) \quad \Big((a|b \wedge b|c) \;\; \Longrightarrow \quad a|c\Big)$$

### 1.4.3 Notion de Diviseur Commun

Soient $a$ et $b$ deux entiers naturels nuls.
On dit que l'entier $d$ est un diviseur commun à $a$ et à $b$ si et seulement si $d$ est un diviseur à la fois de $a$ et de $b$.
En d'autres termes, $d$ est un diviseur commun à $a$ et à $b$ si et seulement si

$$(\exists(k, k') \in \mathbb{N}) \quad : \quad a = kd \quad \text{et} \quad b = k'd.$$

**Exemple 13.** 3 est un diviseur commun à 12 et à 21 car $12 = 4 \times 3$ et $21 = 7 \times 3$.

7 est un diviseur commun à 14 et à 21 car $14 = 2 \times 7$ et $21 = 3 \times 7$.

**remarque 14.**

*REMARQUE IMPORTANTE*

*Si $d$ est un diviseur commun à $a$ et à $b$ alors $d$ est un diviseur de toute combinaison linéaire de $a$ et $b$.*

*Ce qui revient à dire que*

$$\boxed{d|a \ \ et \ \ d|b \quad \Longrightarrow \quad (\forall(\lambda,\mu) \in \mathbb{N}^2) \quad d \mid (\lambda a + \mu b)}$$

*Par exemple, 7 comme diviseur de 14 et 21, sera automatiquement un diviseur de la combinaison $2.14 + 3.21 = 91$*

*Cette remarque sera d'une grande utilité dans la preuve de la réciproque du théorème de Bezout, à venir.*

### 1.4.4 Plus Grand Commun Diviseur : pgcd

Soient $a$ et $b$ deux entiers naturels et $D_a$ ( resp. $D_b$ ), l'ensemble des diviseurs de $a$ ( resp. de $b$.)

On a

1. $D_a \cap D_b \neq \emptyset$ car $1 \in D_a \cap D_b$

2. $\max D_a = a$ et $\max D_b = b$

3. $1 \leq \max D_a \cap D_b \leq \max(a, b)$.

On en déduit que l'ensemble $D_a \cap D_b$ est une partie finie de $\mathbb{N}$ qui admet nécessairement un plus grand élément, appelé plus grand diviseur commun de $a$ et $b$ et noté $pgcd(a, b)$ ou parfois $(a \wedge b)$.

**Exemple 15.** Prenons $a = 36 = 2.2.3.3$ et $b = 30 = 2.3.5$ .

$$D_a = \{1, 2, 3, 4, 6, 9, 12, 18, 36\} \quad \text{et} \quad D_b = \{1, 2, 3, 5, 6, 10, 15, 30\}$$

Donc

$$D_a \cap D_b = \{1, 2, 3, 6\}$$

et

$$pgcd(36, 30) = \max D_a \cap D_b = 6$$

### 1.4.5 Plus Petit Commun Multiple : ppcm

Soient $a$ et $b$ deux entiers naturels et $M_a$ (resp. $M_b$), l'ensemble des multiples de $a$ (resp. de $b$.)

On a

1. $M_a \cap M_b \neq \emptyset$ car $ab \in M_a \cap M_b$
2. $\min M_a = a$ et $\min M_b = b$
3. $\max M_a \cap M_b \geq ab$.

On en déduit que l'ensemble $M_a \cap M_b$ admet un plus petit élément, appelé plus petit multiple commun de $a$ et $b$ et noté $ppcm(a, b)$.

**Exemple 16.** Prenons $a = 42 = 2.3.7$ et $b = 48 = 2.3.8$ .

$$M_a = \{42, 84, 126, 168, 210, 252, 294, 336, 378...\} \quad \text{et} \quad M_b = \{48, 96, 144, 192, 240, 288, 336, ...\}$$

Donc

$$M_a \cap M_b = \{336, ....\}$$

et

$$ppcm(42, 48) = \min M_a \cap M_b = 336$$

Dans tout ce qui va suivre, on mettra de côté cette notion de multiple, car lorsqu'il s'agit de très grands nombres, le ppcm est certainement très grand, alors que le pgcd pourrait rester suffisamment petit et donc facilement manipulable.

### 1.4.6 Lemme d'Euclide : Base des autres théorèmes

Ce lemme, malgré sa simplicité, se trouve être à la base de l'algorithme d'Euclide, de l'algorithme d'Euclide étendu, de l'identité de Bezout et en fin du théorème de Bezout.

**Lemme 17.** *Soient $a$ et $b$ deux entiers naturels tels que : $a > b > 0$.*

*On considère l'ensemble $D_1$ (resp. $D_2$) qui contient les diviseurs communs à $a$ et $b$ (resp. à $b$ et $a - b$).*

*On a alors*

$$D_1 \quad = \quad D_2$$

*et par conséquent,*

$$\boxed{\max D_1 \quad = \quad \max D_2 \quad \textit{c'est à dire que} \quad pgcd(a, b) = pgcd(a - b, b)}$$

**démonstration 18.** *Pour montrer que $D_1 = D_2$, nous allons montrer que*

$$D_1 \subset D_2 \quad \textit{et} \quad D_2 \subset D_1.$$

Première inclusion

*Soit $d \in D_1$.*

$$d \in D_1 \implies (\exists (k_1, k_2) \in \mathbb{N}^2) \ : \ a = k_1 d \ et \ b = k_2 d$$

$$\implies (\exists (k_1, k_2) \in \mathbb{N}^2) \ : \ b = k_2 d \ et \ a - b = (k_1 - k_2) d$$

$$\implies (\exists (k_1, k_3) \in \mathbb{N}^2) \ : \ b = k_2 d \ et \ a - b = k_3 d \ avec \ k_3 = k_1 - k_2$$

$$\implies d \in D_2 \quad donc \quad D_1 \subset D_2.$$

*Exactement De la même façon, on montre la deuxième inclusion, c'est à dire que* $D_2 \subset D_1$.

**remarque 19.** *Le lemme ci-dessus permet d'écrire que*

$$pgcd(a, b) = pgcd(a - b, b) = pgcd(a - 2b, b) = pgcd(a - 3b, b) = pgcd(b, a)$$

*Et en particulier, Si* $a = bq + r$ *avec* $0 \leq r < b$, *alors*

$$\boxed{pgcd(a, b) = pgcd(a - b, b) = pgcd(a - 2b, b) = ... = pgcd(a - bq, b) = pgcd(b, r)}$$

*L'application directe de ce lemme conduit à l'algorithme d'Euclide suivant si essentiel en arithmétique.*

### 1.4.7 Algorithme d'Euclide

Soient $a$ et $b$ deux entiers naturels tels que : $a > b > 0$. L'algorithme d'Euclide est une méthode programmable, basé le lemme précédent.

Supposons que la division euclidienne de $a$ par $b$ ait pour résultat :

$$a \ = \ bq_0 \ + \ r_0 \text{ avec } \ 0 \ \leq r_0 \ < b$$

Le lemme ci-dessus, permet d'écrire

$$D = pgcd(a, b) = pgcd(b, a - b) = pgcd(b, a - 2b) = ...pgcd(b, a - bq) = pgcd(b, r_0)$$

de même, si $b = r_0 q_1 + r_1$, alors

$$D = pgcd(b, r_0) = pgcd(r_0, r_1) \quad \text{avec} \quad 0 \leq r_1 < r_0 < b$$

et

$$D = pgcd(r_0, r_1) = pgcd(r_1, r_2) \quad \text{avec} \quad 0 \leq r_2 < r_1 < r_0 < b$$

et ainsi de suite jusqu'a obtenir

$$D = pgcd(r_{N-1}, r_N) \quad \text{avec} \quad 0 \leq r_N < r_{N-1} < ... < r_0 < b$$

$$D = pgcd(r_N, 0) = r_N.$$

car la suite $(r_n)$ est strictement décroissante (jusqu'à 0.)

En d'autres termes, le plus grand diviseur commun de $a$ et $b$ est le DERNIER RESTE NON NUL.

**remarque 20.** *Nous n'avons pas besoin de montrer que*

–
$$(\forall a \in \mathbb{N}^*) \quad pgcd(a, a) = a$$

–
$$(\forall a \in \mathbb{N}^*) \quad pgcd(a, 0) = a$$

–
$$pgcd(0, 0) \quad \textit{ne peut être défini}$$

–
$$(\forall a \in \mathbb{N}) \quad pgcd(a, 1) = 1$$

**Exemple 21.**

$pgcd(72, 30) = pgcd(2.30+12, 30) = pgcd(30, 12) = pgcd(2.12+6, 12) = pgcd(12, 6) = pgcd(6, 0) = 6$

## 1.5 Théorème de Bezout et ses Corollaires

### 1.5.1 Algorithme d'Euclide étendu et Identité de Bezout

Soient $a$ et $b$ deux entiers naturels non nuls tels que $a > b \geq 2$. Alors

$$\boxed{D = \text{ pgcd } (a, b) \quad \Longrightarrow \quad (\exists (u, v) \in \mathbb{Z}^2) \quad : \quad au + bv = D}$$

**démonstration 22.** *La démonstration de l'identité de Bezout, s'obtient en "Remontant " l'algorithme d'Euclide. Supposons que l'on veuille calculer le pgcd $D$ de deux entiers naturels $a$ et $b$ par l'algorithme d'Euclide.*

*On procédera de la manière suivante :*

$$a = bq + r$$
$$b = rq_1 + r_1$$
$$r = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$
$$r_2 = r_3q_4 + r_4$$
$$r_3 = r_4q_5 + r_5$$

•

•

•

$$r_{N-2} = r_{N-1}q_N + r_N$$
$$r_{N-1} = r_N q_{N+1} + 0$$

*Le pgcd est alors*

$$D = r_N.$$

*La remontée de cet algorithme, connue sous le nom d'algorithme étendu se fait ainsi :*

$$r = a - bq = \lambda_0 a + \mu_0 b$$
$$r_1 = b - rq_1 = \lambda_1 a + \mu_1 b$$
$$r_2 = r - r_1 q_2 = \lambda_2 a + \mu_2 b$$
$$r_3 = r_1 - r_2 q_3 = \lambda_3 a + \mu_3 b$$
$$r_4 = r_2 - r_3 q_4 = \lambda_4 a + \mu_4 b$$
$$r_5 = r_3 - r_4 q_5 = \lambda_5 a + \mu_5 b$$

•

•

•

$$r_N = r_{N-2} - r_{N-1}q_N = \lambda_N a + \mu_N b$$

*Conclusion de la remontée de l'Algorithme d'Euclide :*

$$\boxed{pgcd(a,b) = D \quad \Longrightarrow \quad (\exists(\lambda,\mu) \in \mathbb{Z}^2) \ : \ D = \lambda.a + \mu.b}$$

**Exemple 23.** Pour illustrer cette remontée, prenons l'exemple relativement simple suivant :

$$a = 753 \quad \text{et} \quad b = 24$$

L'exécution de l'algorithme de'Euclide donne successivement

$$753 = 24 \times 31 \ + \ 9$$
$$24 = 9 \times 2 \ + \ 6$$
$$9 = 6 \times 1 \ + \ 3$$

$$6 = 3 \times 2 \ + \ 0$$

Il s'en suit que le plus petit diviseur commun de 753 et 24 sera 3.

Remontons l'algorithme de la façon suivante :

$$9 = 753 - 31 \times 24$$
$$6 = 24 - 2(753 - 31 \times 24)) = 63 \times 24 - 2 \times 753$$

$$pgcd(753, 24) = 3 = 9 - 6 = 9 - 24 + 9 \times 2 = 3 \times 9 - 24$$
$$= 3(753 - 31 \times 24) - 24 = 3 \times 753 - 94 \times 24.$$

La remontée donne alors

$$\lambda = 3 \quad \text{et} \quad \mu = -94$$

On vérifie bien que

$$3 \times 753 - 94 \times 24 \ = \ 3 = pgcd(753, 24)$$

**remarque 24.** *La réciproque de l'implication précédente, n'est pas toujours vraie. En effet,*

$$12 = 3 \times 8 - 2 \times 6 \ \textit{mais} \quad pgcd\ (8, 6) = 2 \quad \textit{et non pas} \quad 12!$$

En particulier, si $d = 1$, l'implication ci-dessus ( devient l'identité de Bezout) :

$$\boxed{\text{pgcd } (a, b) = 1 \quad \Longrightarrow \quad (\exists (u, v) \in \mathbb{Z}^2) \ : \ au + bv = 1}$$

Dans ce cas précis ($pgcd(a, b) = 1$), la réciproque est vraie. l'implication se transforme alors en une équivalence appélée : Théorème de Bezout.

### 1.5.2 Théorème de Bezout

Ce théorème est vraiment le point de départ de la majorité des théorèmes qui concernent l'Arithmétique des entiers.

Ainsi, les théorèmes de Gauss, d'Euler et de Fermat et leurs applications pratiques en cryptographie, sont issus de façon directe ou indirecte du théorème de Bezout !

Mais avant d'énoncer le théorème de Bezout, commençons par donner la définition primordiale suivante :

**Definition 25.** On dit que deux entiers naturels non nuls sont Premiers entre eux si et seulement si leur plus grand diviseur commun est égal à 1 .

ou bien

On dit que deux entiers naturels non nuls sont Premiers entre eux si et seulement si $D_a \cap D_b = \{1\}$.

ou de façon équivalente,

$$\boxed{a \text{ et } b \text{ sont Premiers entre eux} \iff pgcd(a,b) = 1 \iff D_a \cap D_b = \{1\}.}$$

On vient juste de définir une sorte de relation, qui permettra d'écrire des prédicats, puis des propositions et en fin des théorèmes .

La négation de ce qui précède, nous mène à la définition suivante :

**Definition 26.**

$$\boxed{a \text{ et } b \text{ Ne sont Pas Premiers entre eux} \iff pgcd(a,b) \geq 2 \iff Card(D_a \cap D_b) \geq 2.}$$

Cela veut dire aussi qu'ils ont au moins un diviseur commun supérieur ou égal à 2.

**Théorème 27.**

*Théorème de Bezout*

*Soient $a$ et $b$ deux entiers naturels non nuls voire $\geq 2$. Alors*

$$\boxed{a \text{ et } b \text{ sont premiers entre eux} \iff (\exists (u,v) \in \mathbb{Z}^2) \ : \ au + bv = 1}$$

*OU ce qui revient au même,*

$$\boxed{a \text{ et } b \text{ sont premiers entre eux} \iff (\exists (u,v) \in \mathbb{Z}^2) \ : \ au + bv = -1}$$

**démonstration 28.** *La condition est nécessaire* : $\Longrightarrow$

*Il suffit d'appliquer l'identité de Bezout, sachant que $pgcd(a,b) = 1$.*

*La condition est suffisante* : $\Leftarrow$

*Supposons que :* $(\exists (u,v) \in \mathbb{Z}^2) \ : \ au + bv = 1$.

*Soit $d$ un diviseur commun à $a$ et à $b$.*

*$d$ sera alors un diviseur de la combinaison $au + bv$.*

*Or $au + bv = 1$ donc forcément $d = 1$.*

*Il s'en suit que 1 est le seul diviseur commun à $a$ et à $b$.*

*Ce qui veut dire que $a$ et $b$ sont premiers entre eux.*

*CQFD.*

**Exemple 29.** Si $a$ est un entier $\geq 1$
$a$ et $2a-1$ sont premiers entre eux, car $2.a - (2a-1) = 1$.

Cas Particulier

1. Si le reste de la division Euclidienne de $a$ par $b$ est égal à 1 , alors $a$ et $b$ sont premiers ente eux.
2. Si le reste de la division Euclidienne de $a$ par $b$ est égal à $b-1$ , alors $a$ et $b$ sont premiers ente eux.
3. $(\exists (u,v) \in \mathbb{Z}^2) \quad : \quad au + bv = -1 \iff pgcd(a,b) = 1.$
4. $(\forall a \geq 1)$ $a$ et $a+1$ sont premiers entre eux
5. $(\forall a \geq 2)$ $a$ et $a-1$ sont premiers entre eux

**remarque 30.** *En prenant la négation du théorème de Bezout, on obtient l'équivalence*

$$\boxed{a \text{ et } b \text{ NE sont PAS premiers entre eux} \iff (\forall (u,v) \in \mathbb{Z}^2) \quad : \quad au + bv \neq 1}$$

**Corollaire 31.** *Soient $a, m, n$ trois entiers naturels non nuls.*

$$\boxed{pgcd(a,m) = 1 \quad et \quad pgcd(a,n) = 1 \quad \iff \quad pgcd(a,mn) = 1}$$

Ce résultat intermédiaire nous sera d'une grande utilité par la suite, en particulier dans la démonstration du théorème d'Euler.

Sa démonstration, basée sur le théorème de Bezout, est laissée au lecteur en guise d'exercice.

Voici maintenant un exemple d'application de l'Algorithme étendu et du théorème de Bezout.

### 1.5.3 Résolution des équations Diophantiennes

Etant donnés trois entiers naturels $a, b$ et $d$, On appelle équation diophantienne, toute équation de la forme :

$$\boxed{ax + by = d}$$

Les inconnues $x$ et $y$ sont des entiers relatifs.

1. Existence d'une solution

   Si une solution $(x, y)$ existe, alors nécessairement

   $$pgcd(a,b)|d \quad \text{car} \quad pgcd(a,b)|ax \quad \text{et} \quad pgcd(a,b)|by$$

   Donc par contraposition, si $pgcd(a,b) \nmid d$, c'est à dire si le pgcd de $a$ et $b$ ne divise pas le second membre $d$ alors, c'est sûr, il n'y aura aucune solution.

   Par exemple, l'équation $6x - 10y = 3$ n'aura aucune solution car

   $pgcd(6, 10) = 2$ et que 2 ne divise pas 3.
2. Cas particulier ( $d = 1$)

   si $pgcd(a,b) \neq 1$, alors il n'y aura pas de solution.

3. Résolution dans le cas $d = 1$ avec $pgcd(a, b) = 1$.

   Il faut d'abord connaître une solution particulière $(x_0, y_0)$.

   On peut trouver Cette solution particulière, en remontant l'Algorithme d'Euclide, c'est à dire grâce à l'identité de Bezout.

   Une autre solution $(x, y)$ , doit forcément satisfaire l'égalité

$$a(x - x_0) = b(y_0 - y)$$

   Le théorème de Gauss permet alors d'écrire

$$x - x_0 = kb \quad \text{et} \quad y_0 - y = ka \quad \text{avec} \quad k \in \mathbb{Z}$$

   d'où la solution générale

$$x = x_0 + kb \quad \text{et} \quad y = y_0 - ka$$

**Exemple 32.** Chercher $(x, y) \in \mathbb{Z}^2$ tel que

$$6x + 15y = 7$$

Le plus petit diviseur commun à 6 et 15 étant égal à 3 et que 3 ne divise pas le second membre 7,

On peut conclure que cette équation n'admet aucune solution.

**Exemple 33.**

$$5x + 7y = 1$$
$$(x_0, y_0) = (-4, 3)$$
$$(x, y) = (-4 + 7k, 3 - 5k), \text{ où } \quad k \in \mathbb{Z}$$

Vérification Prenons $k = -2$ par exemple.

$$(x, y) = (-4 + 7k, 3 - 5k) = (-18, 13)$$
$$5x + 7y = -90 + 91 = 1!$$

Prenons maintenant $k = 2$ .

$$(x, y) = (-4 + 7k, 3 - 5k) = (10, -7)$$
$$5x + 7y = 50 - 49 = 1!$$

### 1.5.4 Théorème de Gauss

En fait, ce théorème n'est qu'une conséquence directe de l'identité de Bezout, mais en même temps, il est d'une grande utilité pour la suite des événements .

Soient $a$, $b$ et $c$ trois entiers naturels non nuls. On a alors

$$\boxed{c|ab \ \wedge \ pgcd(c, a) = 1 \implies c|b}$$

**démonstration 34.**

$c|ab \ \wedge \ pgcd(c,a)=1 \implies$
$(\exists k \in \mathbb{N}) \ : \ ab=kc \ \wedge \ (\exists (u,v) \in \mathbb{Z}^2) \ : \ cu+av=1$
$\implies \ (\exists (u,v) \in \mathbb{Z}^2) \ : \ bcu+abv=b$
$\implies \ \exists (u,v,k) \in \mathbb{Z}^3 \ : \ c(bu+kv)=b$
$\implies \ c|b$
*CQFD.*

Cas Particulier où a est un nombre premier

Soient $b$ et $c$ deux entiers naturels non nuls et $p$ un nombre premier. On a alors

$$\boxed{p|bc \iff p|b \ \vee \ p|c}$$

Cette propriété sera utilisée dans la démonstration du théorème de Wilson vers la fin de ce " polycope".

## 1.6 La Notion de Congruence

Si l'on demande à un mathématicien Ordinaire de calculer à la main le résultat de la division de

791652970064115327666 5 par 9771128453098 , Alors à coup sûr, il mettra beaucoup de temps pour pas grand chose et il se peut même que sa réponse soit incorrecte !

L'arithmétique n'est donc intéressante que si la machine ou l'ordinateur entre en jeu.

Or, comme l'être humain, un ordinateur aussi puissant soit-il, ne peut manipuler que les entiers inférieurs à une certaine limite.

Par exemple, une petite calculette qui utilise uniquement trois (3) bits, ne pourra représenter ou traiter que les nombres

0 codé par 000

1 remplacé par 001

2 traduit par 010

3 symbolisé par 011

4 crypté par 100

5 matérialisé par 101

6 écrit sous la forme 110

7 égal à 111

8 représenté par $000=0$

9 " par $001=1$

$$10 \quad \text{" par} \quad 010 = 2$$

$$11 \quad \text{" par} \quad 011 = 3$$

$$12 \quad \text{" par} \quad 100 = 4$$

$$13 \quad \text{" par} \quad 101 = 5$$

$$14 \quad \text{" par} \quad 110 = 6$$

$$15 \quad \text{" par} \quad 111 = 7$$

$$16 \quad \text{" par} \quad 000 = 8 = 0$$

On dit alors que cette machine manipule les nombres MODULO $8 = 2^3$.

C'est à dire qu'elle ne tient compte que du reste de la division par 8.

Un machine qui code les nombres sur $N$ bits, ne tiendra compte que du reste de la division par $2^N$.

Ceci montre le rôle de la relation de congruence modulo !.

### 1.6.1 Définition

Soient $a$ et $b$ deux entiers relatifs ($\in \mathbb{Z}$) et $n$ un entier naturel $> 1$. On dit que $a$ est congru à $b$ modulo $n$ si et seulement si la différence $a - b$ un multiple de $n$,

Ou si la différence $a - b$ est divisible par $n$,

Ou si $n$ divise la différence $b - a$.

Par définition, On écrira alors

$$a \equiv b \ (\mod n) \iff$$

$$a \equiv b \ [n] \iff$$

$$(\exists k \in \mathbb{Z}) \ : \ a - b = kn \iff$$

$$(\exists k \in \mathbb{Z}) \ : \ a = b + kn \iff$$

$$n|(a - b) \iff$$

$$a - b \text{ est un multiple de } n.$$

**Exemple 35.** $(*)$ $10 \equiv 1 \mod 3$

$(*)$ $10 \equiv -2 \mod 3$

$(*)$ 10 n'est pas congru à 3 mod 3

**Proposition 36.**

| $a \equiv b\ [n] \iff$ *les restes des divisions de* $a$ *et* $b$ *par* $n$ *sont exactement les mêmes.* |
|---|

*Ou, en d'autres termes,*

*$a$ et $b$ sont congrus modulo $n$ , Si et seulement si, ils ont le même reste de la division Euclidienne par $n$ .*

*Cette propriété est très utile pour la suite. Nous en aurons besoin pour démontrer que la fonction indicatrice d'Euler est multiplicative : $\phi(mn) = \phi(m)\phi(n)$ si $pgcd(m,n) = 1$.*

**démonstration 37.** *La condition est Nécessaire*

*Posons $a = nq_1 + r_1$ et $b = nq_2 + r_2$ avec $0 \leq r_1 < n$ et $0 \leq r_2 < n$.*

$$\begin{gathered} a \equiv b[n] \implies \\ n|(a-b) \implies \\ n|(n(q_1-q_2)+r_1-r_2) \implies \\ n|(r_1-r_2) \end{gathered}$$

*or*

$$-n < r_1 - r_2 < n$$

*donc $r_1 - r_2 = 0$.*

*La condition est Suffisante*

$$\begin{gathered} r_1 = r_2 \implies \\ a - nq_1 = b - nq_2 \implies \\ a - b = n(q_1 - q_2) \implies \\ a \equiv b[n]. \end{gathered}$$

**remarque 38.**

1. *La proposition ci-dessus permet de vérifier très facilement que La congruence est une relation d'équivalence.*

2. *La classe d'équivalence de $a$ modulo $n$ contiendra tous les entiers relatifs de la forme $a + kn$ où $k \in \mathbb{Z}$*

3. *La classe d'équivalence de $0$ modulo $n$ contiendra tous les multiples de $n$.*

4. *Si $n = 7$ , alors $\overline{3} = \{..., -18, -11, -4, 3, 10, 17, 24, ...\} = \overline{10}$*

5. *Si $n = 5$ , alors $\overline{3} = \{..., -12, -7, -2, 3, 8, 13, 18, ...\} = \overline{13}$*

6. *L'ensemble quotient de la congruence modulo $n$ est noté $\mathbb{Z}/n\mathbb{Z}$.*
   *Il est constitué uniquement des restes de la division par $n$ , que l'on appelle les représentants :*

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, 3, ..., n-1\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, ..., \overline{n-1}\}$$

### 1.6.2 Compatibilité de la congruence avec l'addition

**Proposition 39.**

$$(\forall (a,a',b,b') \in \mathbb{Z}^4) \ \ (\forall n \in N^*)$$

$$\boxed{a \ \equiv \ b \ \ [n] \quad et \quad a' \equiv b' \ \ [n] \quad \Longrightarrow \quad a+b \equiv a'+b' \ \ [n]}$$

**démonstration 40.** $a \equiv b \mod n \implies (\exists k \in \mathbb{Z}) \ : \ a = b + \ kn$

$a' \equiv b' \mod n \implies (\exists k' \in \mathbb{Z}) \ : \ a' = b' + \ k'n$

$\implies (a+a') = (b+b') + (k+k')n$

$\implies (\exists k'' = k + k' \in \mathbb{Z}) \ : \ (a+a') = (b+b') + k''n$

$\implies a + b \equiv a' + b' \mod n.$

### 1.6.3 Compatibilité de la congruence avec la multiplication

**Proposition 41.**

$$(\forall (a,a',b,b') \in \mathbb{Z}^4) \ \ (\forall n \in N^*)$$

$$\boxed{a \ \equiv \ b \ \ [n] \quad et \quad a' \equiv \ b' \ \ [n] \quad \Longrightarrow \quad ab \equiv a'b' \ \ [n]}$$

**démonstration 42.** $a \equiv b \mod n \implies (\exists k \in \mathbb{Z}) \ : \ a = b + \ kn$

$a' \equiv b' \mod n \implies (\exists k' \in \mathbb{Z}) \ : \ a' = b' + \ k'n$

$\implies aa' = bb' + (kb' + k'b + kk'n)n$

$\implies (\exists k'' = kb' + k'b + kk'n \in \mathbb{Z}) \ : \ aa' = bb' + k''n$

$\implies ab \equiv a'b' \mod n.$

### 1.6.4 Compatibilité de la congruence avec la puissance

**Corollaire 43.**

$$(\forall (a,b) \in \mathbb{Z}^2) \ \ (\forall n \in N^*)$$

$$\boxed{a \ \equiv \ b \ \ [n] \quad \Longrightarrow \quad (\forall p \in \mathbb{N}^*) \ \ a^p \equiv b^p \quad [n]}$$

*Cette propriété est très pratique, en particulier lorque $b = \pm 1$.*

**Exemple 44.** Pour calculer le reste de la division de $2019^{2017}$ par 4, il suffit de remarquer que

$$2019 \ \equiv \ -1 \quad \mod 4$$

et par suite

$$2019^{2017} \equiv (-1)^{2017} \equiv -1 \equiv 3 \mod 4$$

Le reste sera donc égal à 3 .

### 1.6.5 L'anneau quotient $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Soit $n$ un entier naturel tel que $n > 1$.

On a vu que l'ensemble noté $\mathbb{Z}/n\mathbb{Z}$ représente l'ensemble quotient de la relation de congruence modulo $n$, ou aussi l'ensemble des classes d'équivalence de cette même congruence.

Ainsi, l'ensemble quotient ne contiendra que les classes des restes de la division par $n$, étant donné que deux nombres qui ont le même reste par $n$ , seront dans la même classe d'équivalence.

On a alors

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$$

Connaissant les éléments de cet ensemble, nous allons le munir d'une loi additive + et d'une loi multiplicative $\times$ de la façon suivante :

$$(\forall(\overline{a}, \overline{b}) \in (\mathbb{Z}/n\mathbb{Z})^2) \quad \overline{a} + \overline{b} = \overline{a+b}$$

et

$$(\forall(\overline{a}, \overline{b}) \in (\mathbb{Z}/n\mathbb{Z})^2) \quad \overline{a} \times \overline{b} = \overline{a \times b}$$

Il est très facile de vérifier que :

1. $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien, avec $\overline{0}$ comme élément neutre.

2. La multiplication est associative et admet $\overline{1}$ comme élément neutre (unité).

3. La multiplication est distributive par rapport à l'addition ;

On dit alors que le système $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau ou a une structure d'anneau.

**remarque 45.** *Les propositions suivantes sont très utiles et très pratiques.*

1) *Pour qu'un "anneau" devienne un "corps", il faut que tous les éléments non nuls (autres que l'élément neutre de l'addition), soient inversibles (relativement à la loi multiplicative.)*

2) *Un élément non nul* $\overline{a}$ *de* $\mathbb{Z}/n\mathbb{Z}$ *est inversible si et seulement si*

$$(\exists \overline{a'} \in \mathbb{Z}/n\mathbb{Z}) \quad \overline{a}\overline{a'} = \overline{1} \quad ou \quad aa' \equiv 1 \mod n$$

*Par exemple, dans* $\mathbb{Z}/5\mathbb{Z}$ *, l'inverse de* 3 *est* 2 *car* $2 \times 3 = 6 \equiv 1 \mod 5$

3) *Dans l'anneau* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *, un élément non nul a est inversible si et seulement si*

*il est premier avec $n$ . C'est une conséquence directe du théorème de Bezout.*

4) *Par conséquent, Dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ , un élément non nul a N'est Pas inversible si et seulement si*

*il N'est Pas premier avec $n$ c'est à dire qu'il a un diviseur commun $\geq 2$ avec $n$ .*

5) *En particulier, Si $p$ est un nombre premier, alors tous tous les entiers compris entre* 1 *et $p-1$ sont premiers avec $p$. Il s'en suit que tous les éléments non nuls de $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ sont inversibles.*

$$\boxed{p \text{ est premier} \iff (\mathbb{Z}/p\mathbb{Z}, +, \times) \text{ est un corps commutatif}}$$

# Chapitre 2

# Notion de Primalité dans $\mathbb{N}$

## 2.1 Nombres Premiers

Les nombres premiers sont les briques de l'ensemble $\mathbb{N}$!

Il suffit de connaître les nombres premiers pour connaître les autres nombres naturels .

De nos jours, la répartition de ces nombres premiers reste et restera sûrement pour toujours, un faux mystère .

**Definition 46.** Soit $p$ un nombre entier naturel.

On dit que $p$ est un nombre premier si et seulement si les seuls diviseurs de $p$ sont :

$$1 \quad \text{et} \quad p \quad \text{lui même}$$

Un nombre premier n'est donc divisible que par 1 ET par lui même .

$$(\forall p \in \mathbb{N}) \quad p \text{ est premier} \quad \Longleftrightarrow \quad D_p = \{1, p\}.$$

0 et 1 ne sont pas des nombres premiers . 2 est le plus petit nombre premier.

Pour assuer l'unicité de la décomposition en facteurs premiers de tout naturel non nul, Nous avons évité d'inclure l'unité 1 dans la liste des nombres premiers.

A priori, 1 n'est pas premier!!!

Un nombre premier $p$ ne peut en aucun cas être mis sous la forme d'un produit du type $p = ab$ avec $a \geq 2$ et $b \geq 2$ .

Si un nombre premier $p$ s'écrit sous la forme d'un produit $p = ab$ alors obligatoirement $a = \pm 1$ et $b = \mp p$ ou bien $a = \pm p$ et $b = \mp 1$

**Exemple 47.** 8 n'est pas un nombre premier car 2 est un diviseur de 8 qui est différent et de 1 et de 8.

5 est un nombre premier car 1 et 5 sont ses seuls diviseurs .

La première question qui devrait venir à l'esprit : Combien y a-t-il de nombre premier ??

Pas de suspens, La réponse est immédiate!!

Heureusement, L'homme ne pourra JAMAIS connaître Tous les nombres premiers!!!!!

### 2.1.1 Y a-t-il une infinité de Nombres Premiers ??

Pour répondre à cette question, nous allons avoir besoin des deux lemmes suivants :

**Lemme 48.**

$$\boxed{\textit{Tout entier naturel } n>1 \quad \textit{admet au moins un diviseur premier } p \ : \ 2\leq p\leq n}$$

**démonstration 49.** *Soit $n\in\mathbb{N}^*$. Si $n$ est un nombre premier, on prendra $p=n$.*

*Si $n$ n'est pas premier, alors il se décompose sous la forme d'un produit :*

$$n=n_1.n_2 \ avec \ \ 2\leq n_1<n \quad et \quad 2\leq n_2<n$$

*Si $n_1$ (resp. $n_2$ ) est premier, on prendra $p=n_1(\ resp.n_2)$.*

*Sinon, $n_1$ se décompose à son tour sous la forme :*

$$n_1=n_{11}.n_{12} \quad avec \quad 2\leq n_{11}<n_1<n$$

*On répéte le même processus, jusqu'à obtenir un diviseur premier du type $n_{111\ldots1}\geq 2$ de $n$.*

**Exemple 50.**

$$n=432=16\times 27=n_1.n_2$$
$$n_1=16=4\times 4=n_{11}.n_{12}$$
$$n_{11}=4=2\times 2$$

donc

$$p=n_{111}=2.$$

**Lemme 51.** *Soient $a,b$ et $c$ trois entiers naturels non nuls. Alors*

$$\boxed{a|b \quad et \quad a|(b+c) \quad \Longrightarrow \quad a|c}$$

**démonstration 52.**

$$a|b \quad \Longrightarrow \quad (\exists k_1\in\mathbb{N}) \ : \ b=k_1a$$
$$a|(b+c) \quad \Longrightarrow \quad (\exists k_2\in\mathbb{N}) \ : \ b+c=k_2a$$

*Posons $k_3=k_2-k_1$. On a donc*

$$c=k_3a \ ce \ qui \ se \ traduit \ par \ : \ a|c$$

**Théorème 53.**

*Il existe une Infinité de nombres premiers* !

**démonstration 54.** *Soit $N$ un entier naturel non nul. Raisonnons par l'absurde et supposons que l'ensemble des nombres premiers est fini et contient $N$ éléments.*

*Soit $E = \{p_1, p_2, p_3, ...p_N\} = \{2, 3, 5, ..., p_N\}$ cet ensemble.*
*Avec l'aide de Dieu, Euclide a eu l'idée " géniale " de considérer le nombre*

$$P = (\ p_1.p_2.p_3...p_N)\ + 1.$$

*D'après le premier lemme ci-dessus, le nombre $P$ qui est $> 1$, doit avoir au moins un facteur premier,*
*c'est à dire qu'il est divisible par au moins un des $p_i$ ou, en d'autres termes,*

$$(\exists i \in 1, 2, 3, ..., N) \quad : \quad p_i | P$$

*Et d'après le deuxième lemme ci-dessus,*

$$p_i | p_1.p_2.p_3, ...p_N \quad et \quad p_i | p_1.p_2.p_3, ...p_N + 1 \quad \Longrightarrow \quad p_i | 1$$

*Ce qui constitue une contradiction car $p_i \geq 2$.*
*La conclusion est donc que l'ensemble des nombres premiers est Infini !*

*Dénotons cet ensemble par $\mathbb{P} = \{2, 3, 5, 7, 11, 13, ...\} = \{p_1, p_2, p_3, ...\}$*

**Lemme 55.**

*Principe de la récurrence forte*

*Soit $P(n)$ un prédicat à une variable de domaine $= \mathbb{N}$ tel que*

1) $P(0)$
2) $(\forall n \geq 0) \quad \Big(P(0) \wedge P(1) \wedge ...P(n) \quad \Longrightarrow \quad P(n+1)\Big)$

*Alors*

$$(\forall n \in \mathbb{N}) \quad P(n)$$

A comparer avec la récurrence classique, utilisée d'habitude :

Principe de la récurrence classique

Soit $P(n)$ un prédicat à une variable de domaine $= \mathbb{N}$ tel que

1) $P(0)$
2) $(\forall n \geq 0) \quad \Big(P(n) \quad \Longrightarrow \quad P(n+1)\Big)$

Alors

$$(\forall n \in \mathbb{N}) \quad P(n)$$

et

Principe de la récurrence médiane :

Soit $P(n)$ un prédicat à une variable de domaine $= \mathbb{N}$ tel que

1) $P(0)$
2) $(\forall n \geq 0) \quad \Big((P(n-1) \wedge P(n)) \quad \Longrightarrow \quad P(n+1)\Big)$

Alors

$$(\forall n \in \mathbb{N}) \quad P(n)$$

Il est clair que :

| La récurrence classique $\Longrightarrow$ La récurrence médiane $\Longrightarrow$ La récurrence forte |
|---|

### 2.1.2 Théorème fondamental de l'arithmétique

| Tout entier naturel $\geq 4$ se décompose de façon unique |
|---|

| en un produit de puissances de facteurs premiers |
|---|

Par exemple : $720 = 2^4.3^2.5$

**démonstration 56.** *Montrons d'abord, l'existence de cette décomposition, c'est à dire que que*

$$(\forall n \geq 4) \quad P(n)$$

*avec*

$$P(n) \quad : \quad (\exists \alpha_1, \alpha_2, ... \in \mathbb{N}) \quad : \quad n = \prod_{p_i \in \mathbb{P}} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} ...$$

*Ensuite, on montrera que cette décomposition est unique.*

*Utilisons la récurrence forte.*

*Initialisation*

$$4 = 2^2 \quad \Longrightarrow \quad P(4)$$

*Hérédité*

*Soit $n \geq 4$ tel que $P(n)$.*
*Si $n+1$ est premier, alors $n+1 = p_1^1$ avec $p_1 = n+1$ donc $P(n+1)$.*
*Si $n+1$ n'est pas premier, alors $n+1$ admet au moins deux diviseurs $a$ et $b$ tels que*

$$1 < a < n+1 \text{ et } 1 < b < n+1 \text{ et } n+1 = ab$$

*Donc, d'après l'hypothèse de la récurrence forte,*

$$a = \prod_{p_i \in \mathbb{P}} p_i^{\beta_i}$$

*et*

$$b = \prod_{p_i \in \mathbb{P}} p_i^{\gamma_i}$$

*par suite*

$$n+1 = ab = \prod_{p_i \in \mathbb{P}} p_i^{\beta_i + \gamma_i} = \prod_{p_i \in \mathbb{P}} p_i^{\alpha_i}$$

*avec $\alpha_i = \beta_i + \gamma_i$.*
*CQFD.*

*Vérifions l'unicité d'une telle factorisation*

*Soit $n$ un entier naturel $\geq 4$. Supposons que*

$$n = \prod_{p_i \in \mathbb{P}} p_i^{\alpha_i} = \prod_{p_i \in \mathbb{P}} p_i^{\alpha'_i}$$

*Le théorème de Gauss, nous permet de conclure que*

$$p_1^{\alpha_1} | p_1^{\alpha'_1} \quad \text{et que} \quad p_1^{\alpha'_1} | p_1^{\alpha_1}$$

*Ce qui veut tout simplement dire que $\alpha_1 = \alpha'_1$. De la même façon, on vérifie que $\alpha_i = \alpha'_i$ pour tout $i \in \mathbb{N}$.*

**remarque 57.**

*Pourquoi 1 n'est pas premier ?*

*On a, par exemple,*
$15 = 1^2.3.5 = 1^4.3.5 = 1^7.3.5 = 3.5$
*Donc pour rendre UNIQUE, la décomposition d'un entier en produit de facteurs premiers, Il a été décidé que*
*le nombre 1 n'était pas un nombre premier, Si bien que le plus petit nombre premier est* 2!

### 2.1.3 Un test de primalité : Le Théorème de Wilson

**Lemme 58.** *Pour tout entier naturel $n$ non nul, on a*

$$(n-1)^2 \equiv 1 \mod n$$

*En d'autre termes, $n-1$ est son propre inverse relativement à la multiplication modulo $n$.*

**démonstration 59.** *Il suffit de remarquer que* $n^2+2n \equiv 0 \mod n$ *et que* $(n+1)^2 = n^2+2n+1$.

**Exemple 60.** Prenons $n = 8$ et $m = 12$ .

$$(n-1)^2 = 49 = 6.8+1 \implies (n-1)^2 \equiv 1 \mod n$$

$$(m-1)^2 = 121 = 10.12+1 \implies (m-1)^2 \equiv 1(\mod m)$$

**Lemme 61.** *Soit $p$ un nombre premier.*

$$\boxed{(\forall x \in \mathbb{N}) \quad x^2 \equiv 1 \mod p \iff x \equiv 1 \text{ ou } x \equiv -1 \mod p}$$

**démonstration 62.** *Soit $x \in \mathbb{N}$.*

$$x^2 \equiv 1 \mod p \implies$$
$$(x-1)(x+1) \equiv 0 \mod p \implies$$
$$p \text{ divise le produit } (x-1)(x+1) \implies$$
$$pgcd(p, x-1) \neq 1 \text{ ou } pgcd(p, x+1) \neq 1 \implies$$
$$p \text{ divise } (x-1) \text{ ou } p \text{ divise } (x+1)\ , \implies$$
$$(x-1) \equiv 0 \text{ ou } (x+1) \equiv 0 \mod p \implies$$
$$x \equiv 1 \text{ ou } x \equiv -1 \mod p$$

*CQFD.*

**remarque 63.** *Le résultat précédent n'est pas valable si $p$ n'est pas premier.*
*En effet, si l'on prend $p = 8$, alors on a*

$$3^2 \equiv 1 \mod p \text{ alors que } 3 \neq 1 \text{ et } 3 \neq -1$$

Théorème de Wilson

Ce théorème offre une condition nécessaire et suffisante pour qu'un entier soit premier. Il constitue ce qu'on appelle un test ou critère de primalité.

**Théorème 64.**

$$\boxed{\boxed{p \text{ premier} \iff (p-1)! \equiv -1 \mod p}}$$

**démonstration 65.**

$\underline{\Longrightarrow \text{ : } \textit{La condition est nécessaire}}$

*Si $p$ est premier alors $1, 2, 3, ..., p-1$ sont inversibles.*
*Or l'inverse de $1 = 1$ et l'inverse de $p-1 = p-1$ et d'après le lemme juste ci-dessus,*
*$1$ et $p-1$ sont les seuls nombres entre $1$ et $p-1$ inversibles et EGAUX à leurs inverses.*
*Par conséquent, chaque nombre situé entre $2$ et $p-1$ est différent de son inverse. Il s'en suit que*

$$2.3.4...(p-2) = 1 \mod p$$

*d'où, en multipliant par $p-1$,*

$$1.2.3...(p-2).(p-1) \equiv (p-1) \equiv -1 \mod p$$

$\underline{\Leftarrow \text{ : } \textit{La condition est suffisante}}$

*Montrons la contraposée.*
*Si $p$ n'est pas premier, alors $p = ab$ avec $2 \leq a < p-1$ et $2 \leq b < p-1$.*
*Distinguons deux cas*
$\underline{a \neq b}$
*on aura alors*

$$(p-1)! = 1.2.3...(p-2).(p-1) = 1....a...b...(p-1) \equiv 0 (\neq -1) \mod p$$

$\underline{a = b}$
*Puisque $a^2 \equiv 0_m odp$, On aura*

$$[(p-1)!]^2 = [1.2.3...a...(p-1)].[1.2.3...a...(p-1)] \equiv 0 \mod p$$

*On en déduit que*

$$(p-1)! \neq -1 \mod p$$

*car si*
$(p-1)! \equiv -1 \mod p$, *on aurait*
$[(p-1)!]^2 \equiv 1 \mod p$ *au lieu de* $0$.

**Exemple 66.** avec $p = 5$ premier, on aura

$$(p-1)! = 2.3.4 = 24 \equiv -1 \mod 5$$

et avec $p = 7$ premier, on aura

$$(p-1)! = 2.3.4.5.6 = 720 \equiv -1 \mod 7$$

**Exemple 67.** avec $p = 6$ Non premier, on aura

$$(p-1)! = 2.3.4.5 = 120 \equiv 0 \mod 6$$

et avec $p = 4$, Non premier, on aura

$$(p-1)! = 2.3 = 6 \equiv 2 \mod 8$$

### 2.1.4 Lien entre nombres premiers et Fonction " Dzéta ($\zeta$) " de Riemann

Soit $\mathcal{P}$ l'ensemble infini des nombres premiers et $s$ un nombre complexe tel que : $|s| > 1$ .

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \sum_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$$

Ce lien entre la fonction dzéta de Riemann et la Répartition des nombres premiers explique pourquoi les mathématiciens se battent jour et nuit pour démontrer la conjecture à $10^6$ Dollards, connue sous le nom de " Hypothèse de Riemann "(Voir Google), qui prétend que les zéros de la fonction dzéta ont TOUS une PARTIE REELLE $= \frac{1}{2}$!!!

$$\boxed{\text{Conjecture à 1000000 Dollards} \quad : \quad \zeta(z) = 0 \iff \mathcal{R}e(z) = \frac{1}{2}}$$

## 2.2 Indicateur ou Fonction indicatrice d'Euler et application à la cryptographie

C'est une fonction essentielle en arithmétique et en théorie des nombres. Elle est intimement liée à la répartition des nombres premiers, qui jouent un rôle important dans tout ce qui est en liaison avec le codage, le cryptage, le décodage, la sécurité informatique, ...

**Definition 68.** Soit $n$ un entier naturel non nul. L'indicateur d'Euler ou la fonction indicatrice d'Euler, notée $\phi(n)$, associe à $n$ le nombre d'entiers compris entre 1 et $n$ qui sont premiers avec $n$.

$$(\forall n \in \mathbb{N}^*) \quad \phi(n) = Card\{k \in \mathbb{N} \ : \ 1 \leq k < n \text{ et } \ pgcd(k, n) = 1\}$$

**Exemple 69.**

$$\phi(8) = Card\{1, 3, 5, 7\} = 4 = 7 - Card\{2, 4, 6\}$$
$$\phi(16) = Card\{1, 3, 5, 7, 9, 11, 13, 15\} = 8 = 15 - Card\{2, 4, 6, 8, 10, 12, 14\}$$
$$\phi(11) = Card\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = 10 = 10 - Card\{\}$$

– – – – – – – – – Remarque plus ou moins importante – – – – – – – – – – – – – –

$$\boxed{(\forall n \in \mathbb{N}^*) \quad \phi(n) = \#\{m \in \mathbb{N} \quad : 1 \leq m \leq n \ \wedge \ (\exists i \in \mathbb{N}) \ : \ im \equiv 1 \mod n\}}$$

Autrement dit, $\phi(n)$ représente le nombre des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles!!

**Exemple 70.** Prenons le cas $n = 10$. On a

$$1.1 \equiv 1 \mod 10$$
$$3.7 \equiv 1 \mod 10$$
$$7.3 \equiv 1 \mod 10$$

$$9.9 \equiv 1 \mod 10$$

Il y a donc 4 éléments de $\mathbb{Z}/10\mathbb{Z}$ qui sont inversibles. Par conséquent

$$\phi(10) = 4.$$

**remarque 71.** *On verra plus loin que l'on peut calculer* $\phi(10)$ *sachant que* $10 = 2.5$ *par la formule* $\phi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5}) = 4$

### 2.2.1 Propriétés de la fonction indicatrice

***Cas où*** $n$ ***est un nombre premier*** $p$.

$$\phi(p) = p - 1$$

**démonstration 72.** *Si* $p$ *est un nombre premier, cela veut dire que les seuls diviseurs de* $p$ *sont* $1$ *et* $p$ *lui même.*

*Un nombre strictement inférieur à* $p$ *ne peut avoir* $p$ *comme diviseur, donc un nombre strictement inférieur à* $p$ *est forcément premier avec* $p$.

*Il s'en suit que tous les entiers compris, de façon large, entre* $1$ *et* $p - 1$ *sont premiers avec* $p$.

*d'où l'implication*

$$\boxed{p \text{ premier} \quad \Longrightarrow \quad \phi(p) = p - 1}$$

***Cas du produit*** $mn$ ***où*** $m$ ***et*** $n$ ***sont premiers entre eux***

$$\boxed{m \quad \text{et} \quad n \quad \text{premiers entre eux} \quad \Longrightarrow \quad \phi(mn) = \phi(m).\phi(n)}$$

**démonstration 73.** *Il s'agit de comptabiliser les nombres compris entre* $1$ *et* $mn$ *qui sont premiers avec* $mn$.

*Tout entier naturel* $a$ *situé entre* $1$ *et* $mn$, *peut s'écrire sous la forme* $a = lm + r$ *avec* $0 \leq l \leq n - 1$ *et* $1 \leq r \leq n$.

*Par exemple si* $m = 3$ *et* $n = 5$, *alors les nombre* $6$ *et* $11$ *s'écriront*

$$6 = m + 3 \quad et \quad 11 = 3m + 2.$$

*Mais d'après le Lemme d'Euclide, on a* $pgcd(a, m) = pgcd(lm + r, m) = pgcd(r, m)$.

*Or, par définition de la fonction d'Euler, il y a* $\phi(m)$ *entiers entre* $1$ *et* $m - 1$ *qui sont premiers avec* $m$ .

*Les nombres qui sont entre* $1$ *et* $mn$ *qui sont premiers avec* $m$ *sont de la forme*

$lm + r$ *où* $r$ *est premier avec* $m$ *car* $pgcd(a, m) = pgcd(r, m)$ *et* $0 \leq l \leq n - 1$.

*Maintenant, il faut remarquer que pour un tel* $r$,

$$l \neq l' \quad \Longrightarrow \quad lm + r \neq l'm + r \mod (n)$$

*Car, en effet,*

$$lm+r = l'm+r \mod (n) \implies (l-l')m = 0 \mod (n) \implies l = l' \ car \ pgcd(m,n) = 1$$

*puisque d'après le théorème de Gauss, on aurait* $n|(l-l')$ *avec* $|l-l'| < n$.
*On en déduit que, pour chaque* $r \in \{1,2,3,...,n\}$ *premier avec* $n$*, les nombres de la forme* $lm+r$ *avec* $0 \leq l \leq n-1$ *sont deux à deux distincts modulo* $n$.
*Donc parmi ces* $n$ *nombres, il y en a* $\phi(n)$ *qui sont premiers avec* $n$.

*conclusion*

*Il y a* $\phi(m)$ *nombres premiers avec* $m$ .
*Pour chacun de ces nombres, il y en a* $\phi(n)$ *qui sont premiers avec* $n$ .
*Donc il y a* $\phi(m)\phi(n)$ *nombres premiers avec* $mn$ .

***Cas du produit de deux nombres premiers différents*** $p$ ***et*** $q$.

$$\boxed{\phi(pq) = \phi(p).\phi(q) = (p-1)(q-1)}$$

Cette formule est à la base du cryptage qui utilise le protocole RSA (V. Google)

**démonstration 74.** *Si* $p$ *et* $q$ *sont deux nombres premiers distincts, alors* $p$ *et* $q$ *sont premiers entre eux. On applique alors les deux résultats précédents.*

*Et voici une autre démonstration :*

*Les nombres compris entre* 1 *et* $pq$ *et qui ne sont pas premiers avec* $pq$ *sont les multiples de* $p$*, à savoir* $p, 2p, 3p, ...pq$ *et les multiples de* $q$ *qui sont* $q, 2q, 3q, ...pq$.

*Il y a donc* $q+p-1$ *entiers entre* 1 *et* $pq$ *qui ne sont pas premiers avec* $pq$ .

*Il s'en suit que*

$$\phi(pq) = pq - (q+p-1) = (p-1)(q-1)$$

***Cas d'une puissance d'un nombre premier*** $p$

$$\boxed{(\forall \alpha \in \mathbb{N}^*) \ \ \phi(p^\alpha) = p^\alpha(1-\frac{1}{p})}$$

**démonstration 75.** *Soit* $p$ *un nombre premier et* $\alpha$ *un entier non nul.*

*Les nombres compris entre* 1 *et* $p^\alpha$ *et qui ne sont pas premiers avec* $p^\alpha$ *sont Les multiples de* $p$*, c'est à dire* $p, 2p, 3p, 4p, ...p^{\alpha-1}p$*. Il y en a* $p^{\alpha-1}$.

*Par conséquent*

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1-\frac{1}{p})$$

***Cas général d'un entier naturel*** $n$

Si la décomposition en facteurs premiers de $n$ est de la forme

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}...p_N^{\alpha_N}$$

Alors

$$\boxed{(\forall n \in \mathbb{N}^*)\ \ \phi(n) = n(1 - \frac{1}{p_1}).(1 - \frac{1}{p_2}).(1 - \frac{1}{p_3})...(1 - \frac{1}{p_N})}$$

**démonstration 76.** *Sachant que deux nombres premiers distincts sont évidemment premiers entre eux, et qu'il en est de même de leurs puissances, l'on peut écrire, d'après les résultats ci-dessus, que*

$$\phi(p_1^{\alpha_1}.p_2^{\alpha_2}....p_N^{\alpha_N}) =$$

$$\phi(p_1^{\alpha_1}).\phi(p_2^{\alpha_2})...\phi(p_N^{\alpha_N}) =$$

$$p_1^{\alpha_1-1}(p_1 - 1).p_2^{\alpha_2-1}(p_2 - 1)...p_N^{\alpha_N-1}(p_N - 1) =$$

$$n(1 - \frac{1}{p_1}).(1 - \frac{1}{p_2})...(1 - \frac{1}{p_N}).$$

**Exemple 77.**

$$n = 90 = 2.3^2.5$$
$$\phi(90) = 90(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 24!!!$$

**Lemme 78.** *Soient $a, m, n$ trois entiers naturels. On a alors*

$$pgcd(a, nm) = 1 \iff pgcd(a, n) = 1 \ \ et \ \ pgcd(a, m) = 1$$

**démonstration 79.** 1) *La condition est nécessaire.*
$pgcd(a, nm) = 1 \implies (\exists (u, v) \in \mathbb{Z}^2) \ : \ umn + va = 1$
$\implies (\exists (w, v) \in \mathbb{Z}^2) \ : \ wn + va = 1$
$\implies pgcd(a, n) = 1$
2) *La condition est suffisante.*

**Lemme 80.** *Pour tout entier naturel $n$ et tout entier naturel $a$ premier avec $n$, on a*

$$(\forall r \in \mathbb{N}^*) \quad pgcd(r, n) = 1 \implies pgcd(ar, n) = 1$$

*En fait, ce lemme, a déjà été énoncé sous le nom du corollaire 2 du théorème de Bezout( V. ci-dessus).*

**démonstration 81.** *Raisonnons par l'absurde .*
$pgcd(ar, n) \neq 1 \implies (\exists d > 1) \ : \ d|ar \ et \ \ d|n$
$\implies (\exists (k, k') \in \mathbb{N}^2) \ ar = kd \ et \ \ n = k'd$
$\implies (\exists (k, k') \in \mathbb{N}^2) \ ark' = kdk' = nk$

$\Longrightarrow n|ark'$
$\Longrightarrow n|k'$ *d'après le théorème de Gauss*
$\Longrightarrow k' = n$ *car* $n|k'$ *et* $k'|n$
$\Longrightarrow d = 1$
*Ce qui constitue une contradiction avec* $d > 1$.
*On conclue que* $pgcd(ar, n) = 1$.

### 2.2.2 Théorème d'Euler

Ce théorème, démontré au milieu du $18^{\text{ième}}$ siècle, est resté endormi au placard jusqu'aux années 1970 où l'on a pu découvrir son utilité en cryptographie.

**Théorème 82.**

*Théorème d'Euler*

*Pour tout entier naturel* $n$ *et tout entier naturel* $a$ *premier avec* $n$, *on a*

$$\boxed{a^{\phi(n)} \equiv 1 \quad [n]}$$

*ou, de façon plus académique*

$$\boxed{(\forall (a,n) \in \mathbb{N}^2) \quad \Big( pgcd(a,n) = 1 \quad \Longrightarrow \quad a^{\phi(n)} \equiv 1 \mod n \Big)}$$

**remarque 83.** *Ce théorème, démontré au* $18^{ème}$ *siècle, trouve actuellement de nombreuses applications en Cryptologie( cryptographie + cryptanalyse ), c'est à dire tout ce qui concerne le codage, le décodage, la sécurité de l'information, l'espionnage,... !*

**démonstration 84.** *Soient* $a$ *et* $n$ *deux entiers naturels non nuls Premiers entre eux.*
*Par définition de la fonction* $\phi$ , *entre* $1$ *et* $n$, *il y a* $\phi(n)$ *nombres premiers avec* $n$.
*dénotons par* $r_1, r_2, r_3, ..., r_{\phi(n)}$, *ces nombres.*
*Le génie d'Euler, à l'époque, était de considérer les nombres*

$$ar_1, ar_2, ar_3, ..., ar_{\phi(n)}$$

*et de profiter du fait que, d'après le Lemme ci-dessus (corollaire 2).*

$$(\forall i \in \{1, 2, 3, ..., \phi(n)\}) \quad pgcd(ar_i, n) = 1$$

*Vérifions maintenant que*

$$(\forall (i,j) \in \{1, 2, 3, ..., \phi(n)\}^2) \quad ar_i \equiv ar_j \mod n \quad \Longrightarrow i = j$$

*En effet,*

$$ar_i \equiv ar_j \mod n \quad \Longrightarrow$$
$$a(r_i - r_j) \equiv 0 \mod n \quad \Longrightarrow$$
$$n|a(r_i - r_j) \quad \Longrightarrow$$
$$n|(r_i - r_j) \text{ d'après le théorème de Gauss car } a \text{ est premier avec } n$$

$$\Longrightarrow\ r_i - r_j = 0\ car\ -n < r_i - r_j < n$$
$$\Longrightarrow\quad r_i = r_j.$$

*Il s'en suit que l'ensemble*

$$\{ar_i, i \in \{1, 2, 3, ..., \phi(n)\}\}\ \textit{contient exactement}\ \phi(n)\quad \textit{éléments.}$$

*Cet ensemble est donc égal à*

$$\{r_i, i \in \{1, 2, 3, ..., \phi(n)\}\}$$

*Le produit des éléments de ces deux ensembles sont donc égaux, i.e*

$$r_1.r_2.r_3...r_{\phi(n)} = ar_1.ar_2.ar_3...ar_{\phi(n)} = a^{\phi(n)}r_1.r_2.r_3...r_{\phi(n)}$$

*c'est à dire que*

$$r_1.r_2.r_3...r_{\phi(n)}(a^{\phi(n)} - 1) \equiv 0 \mod n$$

*et en utilisant le théorème de Gauss, sachant que n est premier avec $r_1.r_2, ...r_{\phi(n)}$, On aura*

$$\boxed{a^{\phi(n)} \equiv 1 \mod n}$$

**Exemple 85.** avec

$$n = 4 \quad \text{donc} \quad \phi(4) = 2 \quad \text{et} \quad a = 6$$
$$6^2 = 36 \equiv 0\ [4]$$

car 4 et 6 ne sont pas premiers entre eux.

avec

$$n = 4 \quad \text{donc} \quad \phi(4) = 2 \quad \text{et} \quad a = 7$$
$$7^2 = 49 \equiv 1\ [4]$$

et avec

$$n = 6 \quad \text{donc} \quad \phi(6) = 2 \quad \text{et} \quad a = 11$$
$$11^2 = 121 \equiv 1\ [6]$$

**Lemme 86.** *Soit p un nombre premier, et a un entier naturel non divisible par p.*

*Alors*

$$a \quad et \quad n \quad sont\ premiers\ entre\ eux$$

**démonstration 87.** *p étant un nombre premier, ses seuls diviseurs sont* 1 *et lui même. Si p n'est pas un diviseur de n ou ce qui revient au même, Si n n'est pas un multiple de p, alors le seul diviseur commun à p et à n sera* 1 *. Ce qui traduit le fait que p et n sont premiers entre eux.*

### 2.2.3 Théorème de Fermat

**Théorème 88.**

*Petit Théorème de Fermat*

*Soit $p$ un nombre premier, et $a$ un entier naturel non divisible par $p$.*

*Alors*

$$\boxed{a^{p-1} \equiv 1 \ [p]}$$

**démonstration 89.** *En fait, le petit théorème de Fermat, est une simple conséquence du théorème d'Euler ci-dessus. En effet, si $p$ un nombre premier, et $a$ un entier naturel non divisible par $p$, alors d'une part , d'après le lemme précedent, $a$ et $n$ sont premiers entre eux, et d'autre part, $\phi(p) = p - 1$. Il suffit alors d'applquer le théorème d'Euler.*

**Exemple 90.** avec

$$p = 3 \quad \text{et} \quad a = 6$$

On a

$$6^2 = 36 \equiv 0 \ [3]$$

car $a$ est un multiple de $p$.

**Exemple 91.** avec

$$p = 7 \quad \text{et} \quad a = 2$$

$$2^6 = 64 \equiv 1 \ [7]$$

et avec

$$p = 11 \quad \text{et} \quad a = 2$$

$$2^{10} = 1024 \equiv 1 \ [11] \quad \text{car} \quad 1024 - 1 = 1023 = 93 \times 11$$

### 2.2.4 Le Logarithme discret

C'est un problème plus ou moins difficile qui consiste à, connaissant les entiers $a, b, n$, de trouver l'inconnue $x$ vérifiant :

$$x^a \equiv b \mod n$$

Le protocole RSA largement utilisé dans le cryptage profite de cette difficulté à trouver $x$ connaîssant un certain $x^a$ modulo un certain $n$ notamment lorsqu'il s'agit de très grands nombres.

### 2.2.5 L'algorithme de cryptage RSA

C'est l'une des applications magiques du théorème d'Euler .

### 2.2.6 Comment ça marche ?

Ceci consiste à envoyer un message codé et que seul le récepteur pourra le décoder !
Il se fait en cinq étapes :

1. Le récepteur choisit deux nombres premiers $p$ et $q$ de préférence très très grands.
2. Il calcule leur produit $N = pq$.
3. Il calcule la fonction indicatrice de $N$ par la formule $\phi(N) = (p-1)(q-1)$.
4. Il choisit $e$ ( appelé clé publique) de sorte que $1 < e < \phi(N)$ et $e$ premier avec $\phi(N)$. L'émetteur utilisera ce nombre $e$ pour coder son message.
5. Il garde pour lui $d$ (clé privée ) égal à inverse de $e$ modulo $\phi(N)$. C'est avec $d$ qu'il va décoder le message reçu.

### 2.2.7 Pourquoi ça marche ?

Supposons que l'émetteur veuille envoyer un message constitué de plusieurs caractères. Soit $M$ l'un de ces caractères. l'émetteur connait la clé publique $e$ et le nombre $N$. Il va coder ce caractère en calculant $C = M^e$ modulo $N$ et il envoie le message codé $C$ au récepteur. Ce message codé est publique, c'est à dire qu'il est connu par disons, tout le monde. Etant donné que le récepteur est le seul à connaitre la clé privée $d$, définie par le fait que $d$ est l'inverse de $e$ modulo $\phi(N)$, ce qui veut dire que

$$d.e \equiv 1 \mod \phi(N) \quad \text{ou} \quad d.e = 1 + K.\phi(N) \text{ avec } K \in \mathbb{Z}$$

Rappelons que seul le récepteur connait la valeur de $\phi(N)$. Les autres sont incapable de trouver $\phi(N)$ puisqu'ils n'ont pas les valeurs des nombres premiers $p$ et $q$ tels que : $N = pq$ et $\phi(N) = (p-1)(q-1)$.
Maintenant, il y a deux cas :

$$\underline{M \text{ est premier avec } N}$$

On applique alors le fameux théorème d'Euler qui permet d'écrire

$$M^{\phi(N)} \equiv 1 \mod N \text{ ou aussi } M^{K\phi(N)} \equiv 1 \mod N \text{ pour tout } K \in \mathbb{Z}$$

ou en multipliant par $M$,

$$M^{1+K\phi(N)} = M^{de} = \left(M^e\right)^d \equiv M \mod N$$

$$\underline{M \text{ n' est pas premier avec } N}$$

Etant donné que $N = pq$, et d'après le corollaire 2 du théorème de Bezout, on déduit que

$$M \text{ n'est pas premier avec } p \text{ ou il n'est pas premier avec } q$$

Si $M$ n'est pas premier avec $p$ , alors $M$ est un multiple de $p$ de la forme $\lambda p$ avec $0 \leq \lambda \leq q-1$ car $0 \leq M < pq$.
D'une part, on a

$$\boxed{M \equiv 0 \mod p \implies M^{de} \equiv M \mod p}$$

Et d'autre part, $q$ est premier avec $M$ car $q$ est à la fois premier avec $\lambda$ et avec $p$ et donc $q$ est premier avec leur produit $\lambda.p = M$.

Le théorème d'Euler, s'applique et l'on aura

$$\boxed{M^{q-1} \equiv 1 \mod q \implies M^{(p-1)(q-1)} \equiv 1 \mod q \implies M^{de} \equiv M \mod q}$$

Pour finir, remarquons, à partir des deux encadrés ci-dessus, que $p$ et $q$ sont deux nombres premiers distincts (Donc premiers entre eux), qui divisent $M^{de} - M$.

On en déduit que leur produit $pq$ c'est à dire $N$ divise $M^{de} - M$. Ce dernier résultat se traduit par

$$M^{de} \equiv M \mod N$$

Après le codage ($e$) et le décodage ($d$), on retrouve, heureusement, le message Initial.

**Exemple 92.** Prenons pour simplifier les choses, $p = 2$ et $q = 11$.

Supposons que quelqu'un vous envoie la lettre B représentée par le chiffre 2.

Pour la coder, on a besoin du nombre $e$.

On a

$$N = pq = 33 \text{ et } \quad \phi(N) = \phi(33) = (p-1)(q-1) = 20$$

Choisissons $e < 20$ et premier avec 20. Prenons $e = 3$ par exemple.

Le message codé ou crypté sera alors

$$C = 2^3 \mod 33 = 8$$

Pour le décoder, cherchons $d$ inverse de $e$ modulo $\phi(N) = 20$.

Il faut donc trouver $d$ de sorte que :

$$ed = 3d \equiv 1 \mod 20$$

Pour cet exemple, les calculs sont faciles, on trouve $d = 7$ car $3.7 = 21 \equiv 1 \mod 20$.

Le message Décodé sera alors

$$M = C^d = (8)^7 \mod 33 = (8)^2.(8)^2.(8)^2.8 = (-2).(-2).(-2).8 = 2 = B$$

**Exemple 93.** Prenons maintenant $p = 3$ et $q = 5$.

Supposons que quelqu'un vous envoie la lettre H représentée par le chiffre 8.

Pour la coder, on a besoin du nombre $e$.

On a

$$N = pq = 15 \text{ et } \quad \phi(N) = \phi(15) = (p-1)(q-1) = 8$$

Choisissons $e < 8$ et premier avec 8. Prenons $e = 7$ par exemple.

Le message codé ou crypté sera alors

$$C = 8^7 \mod 15 = 8^2.8^2.8^2.8 = 4.4.4.8 = 4.8 = 2$$

Pour le décoder, cherchons $d$ inverse de $e$ modulo $\phi(N) = 8$.
Il faut donc trouver $d$ de sorte que :

$$ed = 7d \equiv 1 \mod 8$$

Pour cet exemple, les calculs sont faciles, on trouve $d = 7$ car $7.7 = 49 \equiv 1 \mod 8$.
Le message Décodé sera alors

$$M = C^d = (2)^7 \mod 15 = (2)^5.2^2 = 2.4 = 8 = \text{ Message Initial ! } = H$$

Pour être récompensé, Il faut fournir un effort.

Fin.