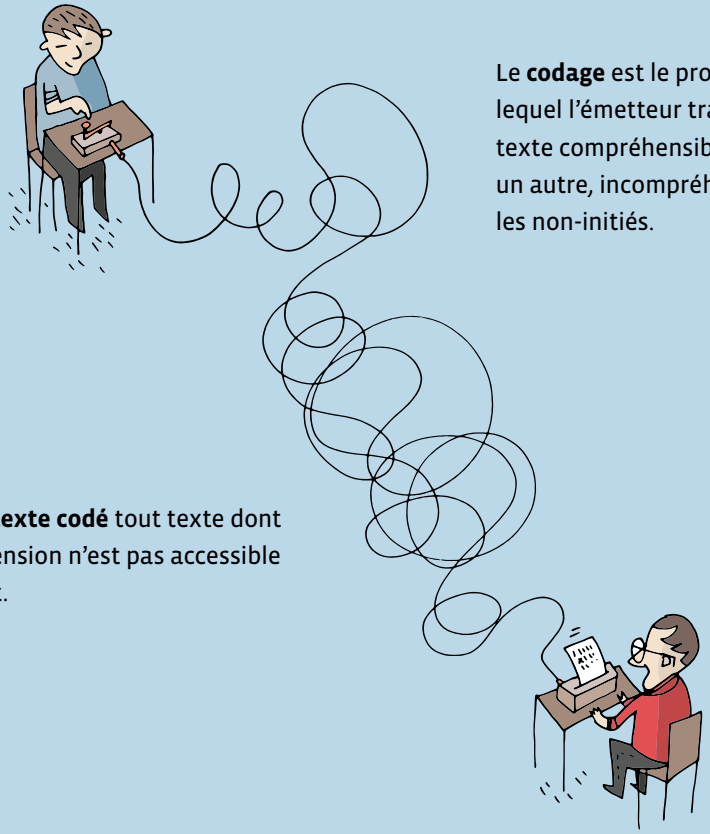
Codes et congruences

Toute communication nécessite la présence d'au moins deux personnes: un **émetteur** et un **récepteur**. Si l'émetteur souhaite que son message ne soit compréhensible que par le récepteur, il doit modifier son texte avant de le transmettre.

On appelle **texte en clair** tout texte dont n'importe qui peut prendre connaissance.



Le **codage** est le procédé suivant lequel l'émetteur transforme un texte compréhensible de tous en un autre, incompréhensible pour les non-initiés.

On appelle **texte codé** tout texte dont la compréhension n'est pas accessible directement.

Le **décodage** est le procédé inverse, utilisé par le récepteur.

La numération

désigne la façon d'écrire les nombres.

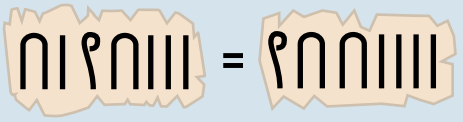
Il existe deux types de numération :

- La **numération additive** : la valeur d'un nombre est égale à la somme des valeurs des symboles qui le composent, indépendamment de leur position dans la représentation du nombre.
- La **numération de position** : la position du symbole dans l'écriture du nombre indique sa valeur.

En réalité, la plupart des numérations sont en partie additive et en partie de position.

La numération égyptienne hiéroglyphique (vers 3000 av. J.-C.)

est une numération uniquement additive.


= 124


= 1

un bâton


= 10

une anse


= 100

une corde enroulée


= 1000

un lotus


= 10 000

un doigt


= 100 000

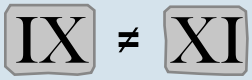
un têtard


= 1 000 000

un dieu

La numération romaine (vers 150 av. J.-C.)

est une numération hybride car les symboles s'additionnent, mais la position du symbole **I** dans l'écriture de **IV** pour 4 ou **VI** pour 6 importe. Il en est de même pour le **X** dans l'écriture de **XC** pour 90 et de **CX** pour 110.




= 1


= 5


= 10


= 50

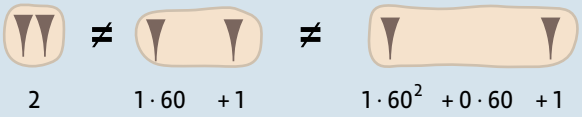

= 100


= 500


= 1000

La numération babylonienne (vers 1800 av. J.-C.)

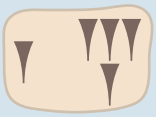
n'est additive que de 1 à 59. Au-delà, elle est de position. Selon leur position dans le nombre, les symboles désignent soit les unités, soit des groupes de 60 unités, ou encore des groupes de $60 \cdot 60$ unités.



$2 \neq 1 \cdot 60 + 1 \neq 1 \cdot 60^2 + 0 \cdot 60 + 1$

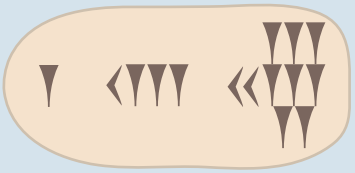
= 1 ou 60 ou 3600

= 10 ou 600 ou 36 000



$1 \cdot 60 + 4$ = 64

$2 \cdot 60 + 40$ = 160



$1 \cdot 60^2 + 13 \cdot 60 + 28$ = 4408

La numération maya (vers 300 av. J.-C.)

n'est additive que pour les nombres de 0 à 19. Elle est ensuite de position, par étage, en utilisant les puissances de 20 à une irrégularité près. En effet, par respect pour l'année solaire, ils utilisaient pour la puissance du troisième étage $18 \cdot 20 = 360$, au lieu de $20 \cdot 20 = 20^2$. Les puissances des étages suivants s'obtiennent bien en multipliant par 20, c'est à dire $18 \cdot 20^2$, $18 \cdot 20^3$, etc.

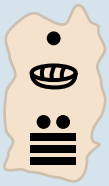
= 1

= 5

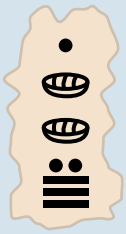
= 0

= 17

$1 \cdot 20 + 17$ = 37



$1 \cdot (18 \cdot 20) + 0 \cdot 20 + 17$ = 377



$1 \cdot (18 \cdot 20^2) + 0 \cdot (18 \cdot 20) + 0 \cdot 20 + 17$ = 7217

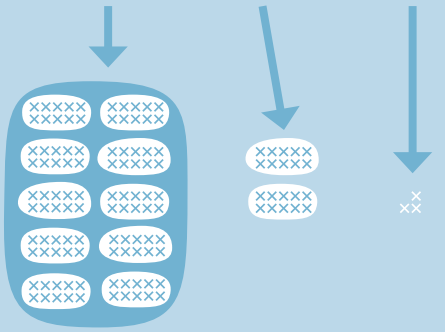
Les numérations modernes

sont des numérations de position: le chiffre 1, par exemple, représente dans notre numération décimale une unité s'il est tout à droite, une dizaine s'il est en deuxième position à partir de la droite, une centaine, s'il est en troisième position à partir de la droite...

Cette façon de représenter les nombres nécessite l'utilisation de bases.

Nous comptons en **base 10** (système décimal). Nous utilisons donc dix chiffres: 0 , 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 et nous effectuons des groupes de dix éléments. Ainsi dix unités forment une dizaine, dix dizaines forment une centaine, dix centaines forment un millier...

$10^3 = 1000$	$10^2 = 100$	$10^1 = 10$	$10^0 = 1$
milliers	centaines	dizaines	unités
0	1	2	3

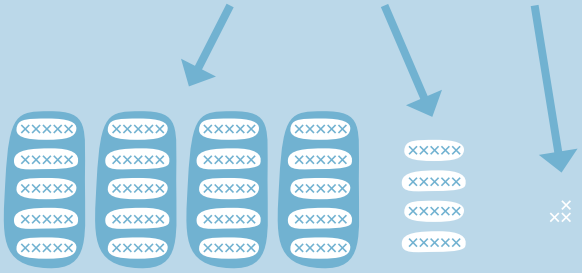


$$123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$$

$$100 \qquad 20 \qquad 3$$

En **base 5**, on utilise cinq chiffres: 0 , 1 , 2 , 3 , 4 . Les groupements se font par cinq, ainsi cinq unités forment un groupe 1 (g^1), cinq groupes 1 forment un groupe 2 (g^2)...

$5^3 = 125$	$5^2 = 25$	$5^1 = 5$	$5^0 = 1$
g^3	g^2	g^1	unités
0	4	4	3



123 se traduit par 443 en base 5

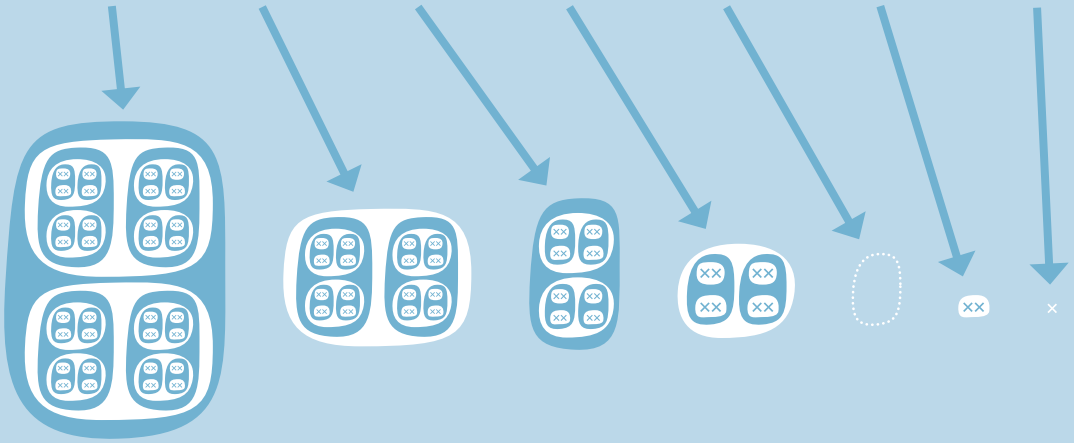
$$123 = 4 \cdot 5^2 + 4 \cdot 5^1 + 3 \cdot 5^0$$

$$100 \qquad 20 \qquad 3$$

Le **code binaire** (en base 2) n'utilise que deux chiffres: 0 et 1. Les groupements se font par deux, ainsi deux unités forment un groupe 1 (g^1), deux groupes 1 forment un groupe 2 (g^2)...

C'est le système de codage qui est utilisé en informatique notamment.

$2^6 = 64$	$2^5 = 32$	$2^4 = 16$	$2^3 = 8$	$2^2 = 4$	$2^1 = 2$	$2^0 = 1$
g^6	g^5	g^4	g^3	g^2	g^1	unités
1	1	1	1	0	1	1



123 se traduit par 1 1 1 1 0 1 1 en base 2

$$123 = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

$$64 \quad 32 \quad 16 \quad 8 \quad 0 \quad 2 \quad 1$$

La congruence modulo *n*

est une curieuse façon de compter qui ne s'intéresse qu'aux restes de la division euclidienne.

Deux nombres entiers ***a*** et ***b*** sont **congrus modulo *n*** si $a - b$ est divisible par ***n*** , ***n*** étant un nombre naturel non nul.
Autrement dit, ***a*** et ***b*** ont le même reste lorsqu'on les divise par ***n***.

On utilise le signe ≡ pour signifier que ***a*** et ***b*** sont **congrus modulo *n***.
Et on note $a \equiv b \pmod{n}$.

13 et 28 sont congrus modulo 5 car:

13	5
reste 3	2

28	5
reste 3	5

On note $13 \equiv 28 \pmod 5$.

La classe de reste $\bar{a}$ modulo *n*

est l'ensemble des nombres qui sont congrus à $a \pmod n$ où ***n*** est un nombre naturel non nul et ***a*** un nombre naturel strictement inférieur à ***n***.

Autrement dit, tous les nombres qui ont pour reste ***a*** lorsqu'on les divise par ***n*** appartiennent à la classe de reste $\bar{a}$ **modulo *n***.

On la note $\bar{a} \pmod n$

$\bar{3} \pmod 5 = \{3 ; 8 ; 13 ; 18 ; 23 ; 28 ; \ldots\}$

Exemple de résolution d'un problème avec restes
Ce genre de problèmes était déjà proposé par le mathématicien chinois Sun Zi (vers 300):

On ignore le nombre de soldats dans les rangs de l'armée chinoise, mais...
- en les comptant 3 par 3, il en reste **2**
- en les comptant 5 par 5, il en reste **3**
- en les comptant 7 par 7, il en reste **1**

Combien y a-t-il de soldats dans les rangs de l'armée chinoise?
Comment résoudre ce système de congruences?
S'il n'en restait aucun après chaque comptage, le nombres de soldats serait un multiple de $(3 \cdot 5 \cdot 7)$.
S'il en restait toujours 1 après chaque comptage, le nombre de soldats serait un multiple de $(3 \cdot 5 \cdot 7)$ auquel on ajouterait 1 soldat.

Enumérons les classes de restes correspondant à chaque proposition:

$\bar{2} \pmod 3 = \{2 ; 5 ; \mathbf{8} ; 11 ; \ldots\}$
$\bar{3} \pmod 5 = \{3 ; \mathbf{8} ; 13 ; 18; \ldots\}$
$\bar{1} \pmod 7 = \{1 ; \mathbf{8} ; 15 ; \ldots\}$

On s'aperçoit que **8** est le plus petit élément commun aux trois classes de restes.

Le nombre de soldats est donc un multiple de $(3 \cdot 5 \cdot 7)$ auquel on ajoute **8** soldats.
L'armée compte **8** soldats ou 113 ou 218 ou ...

Opérations avec les classes de restes

L'addition et la multiplication sont compatibles avec la congruence modulo ***n***.

Par exemple, si nous calculons modulo 5, nous obtenons les résultats suivants:

$\overline{3} + \overline{1} = \overline{4}$ $\quad \overline{3} + \overline{2} = \overline{0}$ $\quad \overline{3} + \overline{3} = \overline{1}$

$\overline{3} \cdot \overline{1} = \overline{3}$ $\quad \overline{3} \cdot \overline{3} = \overline{4}$ $\quad \overline{3} \cdot \overline{0} = \overline{0}$

La preuve par 9

La classe de reste modulo 9 est facile à déterminer en utilisant le critère de divisibilité par 9.
En effet, il est possible de montrer qu'un nombre divisé par 9 donne le même reste que la somme de ses chiffres divisée par 9. Considérons l'exemple suivant:

9542	9
reste 2	1060

$9 + 5 + 4 + 2 = 20$

20	9
reste 2	2

Comme l'addition et la multiplication sont compatibles avec la congruence modulo ***n***, si une opération est fausse, alors son calcul simplifié avec les restes de la division par 9 est également faux.

Vérifions le résultat suivant:

$$26 \cdot 37 \stackrel{?}{=} 963$$
$$\downarrow \quad \downarrow \qquad \downarrow$$
$$\overline{8} \cdot \overline{1} \neq \overline{0}$$

La preuve par 9 est fausse, on en déduit que le produit 963 obtenu en multipliant 26 et 37 est faux.

Attention, une preuve réussie ne signifie pas obligatoirement que le calcul est exact:

Vérifions le résultat suivant:

$$26 \cdot 37 \stackrel{?}{=} 971$$
$$\downarrow \quad \downarrow \qquad \downarrow$$
$$\overline{8} \cdot \overline{1} = \overline{8}$$

La preuve par 9 est réussie, pourtant le produit 971 obtenu en multipliant 26 et 37 est faux, en effet $26 \cdot 37 = 962$.