TS spé

Les congruences

Plan du chapitre :

Avant de commencer le chapitre :

● **Problème motivant l'introduction du chapitre :** calcul du reste de la division euclidienne d'un « grand » entier naturel par 9 (par exemple, pour trouver la clef de contrôle d'un billet de banque)

- Comment peut-on calculer mentalement le reste de la division euclidienne d'un très grand nombre entier par 9 ?
- Comment peut-on le justifier ?

- D'où vient la « preuve par 9 » ? Comment peut-on la justifier ?

● **Vocabulaire :**

congruer : mettre quelque chose en accord

congru/incongru (« portion congrue » dans l'expression)

congruent

● **Historique :**

La notion de congruence est due au mathématicien et physicien allemand **Carl Friedrich Gauss** (1777-1855).

En 1801, Gauss publie les *Disquisitiones Arithmeticae*, un ouvrage consacré à la théorie des nombres (la « reine des mathématiques », selon lui). Cette œuvre majeure au style étonnamment moderne consolide sa réputation. Les trois premiers chapitres forment une introduction à la théorie des congruences où sont développés le petit théorème de Fermat et le théorème de Wilson.

De numerorum congruentia in genere

Ainsi se nomme la première section des *Disquisitiones Arithmeticae*, publiées par Carl Friedrich Gauss en 1801. C'est dans ce texte en latin que l'on trouve pour la première fois les termes francisés en « congru modulo *n* ». Les premiers exemples donnés dans le texte sont les suivants : « – 9 et + 16 secundum modulum 5 sunt congrui ; – 7 ipsius + 15 secundum 11 residuum, secundum modulum 3 vero nonresiduum. » L'adjectif *congruus* qualifie une chose conforme (on retrouve cette idée dans le français *incongru*) et *modulus* signifie *mesure* (on le retrouve dans *modèle* ou dans *moule*). Ainsi, des nombres congrus modulo *n* sont « conformes à la mesure de *n* ».

Dans ce chapitre, toutes les démonstrations sont à connaître.

I. Généralités

1°) Définition

a et b sont deux entiers relatifs.
n est un entier naturel supérieur ou égal à 2.

On dit que les entiers a et b sont **« congrus modulo n »** pour exprimer que leur différence est divisible par n.

On notera que la différence peut être faite dans un sens comme dans l'autre $a-b$ ou $b-a$ (cf. exemple qui suit).

2°) Exemple

$a = 88$
$b = 25$
$n = 3$

a et b sont-ils congrus modulo 3 ?

$a - b = 63$

63 est divisible par 3.

On en déduit que a et b sont congrus modulo 3.

On peut dire que « 88 et 25 sont congrus modulo 3 » ou que « 88 est congru à 25 modulo 3 ».

3°) Notation

On écrit : $a \equiv b \pmod{n}$.

Exemples :

$29 \equiv 1 \pmod 4$ [on lit « 29 est congru à 1 modulo 4 »]

$45 \equiv 0 \pmod 5$

$45 \equiv 5 \pmod 5$

$45 \equiv 10 \pmod 5$

On écrit aussi parfois $a \equiv b \ [\text{mod. } n]$ ou même $a \equiv b \ [n]$.

$a \equiv b \pmod{n}$ signifie que $a - b$ est divisible par n (ou ce qui revient au même $b - a$ divisible par n).

4°) Complément sur la définition

a et b sont deux entiers relatifs.
n est un entier naturel supérieur ou égal à 2.

$$a \equiv b \pmod n \Leftrightarrow n \mid a-b$$
$$\Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } a-b = kn$$
$$\Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } a = b+kn$$

On retient : $a \equiv b \pmod n \Leftrightarrow \exists k \in \mathbb{Z}$ tel que $a = b + kn$.

II. Propriétés immédiates de la relation de congruence (« propriétés des modulos »)

n est un entier naturel supérieur ou égal à 2.
a, b, c sont des entiers relatifs quelconques.

1°) Propriété 1 (réflexivité)

Pour tout entier relatif a, on a :

$a \equiv a \pmod{n}$

Démonstration : évidente

2°) Propriété 2 (symétrie)

Pour tout couple (a, b) d'entiers relatifs.

Si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$.

Démonstration : évidente

3°) Propriété 3 (transitivité)

Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$.

Démonstration :

Par hypothèse, on a : $a \equiv b \pmod n$ donc $a - b$ est divisible par n.

Par hypothèse, on a : $b \equiv c \pmod n$ donc $b - c$ est divisible par n.

Donc la somme $(a-b)+(b-c) = a-c$ est divisible par n.

On en déduit que $a \equiv c \pmod n$.

III. Congruences et opérations algébriques

n est un entier naturel supérieur ou égal à 2.

1°) Propriété 1

a, b, c sont 3 entiers relatifs.

Si $a \equiv b \pmod{n}$, alors $a+c \equiv b+c \pmod{n}$
et $a-c \equiv b-c \pmod{n}$.

Démonstration :

Par hypothèse, on a : $a \equiv b \pmod{n}$.
Donc $a-b$ est divisible par n.

$(a+c)-(b+c)=a-b$

On en déduit que $(a+c)-(b+c)$ est divisible par n.
Par suite $a+c \equiv b+c \pmod{n}$.

2°) Propriété 2

a, b, c, d sont 4 entiers relatifs.

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a+c \equiv b+d \pmod{n}$
et $a-c \equiv b-d \pmod{n}$.

Démonstration :

Par hypothèse, on a : $a \equiv b \pmod{n}$ d'où $a+c \equiv b+c \pmod{n}$.
Par hypothèse, on a : $c \equiv d \pmod{n}$ d'où $b+c \equiv b+d \pmod{n}$.

Par transitivité de la relation de congruence modulo n, on en déduit que $a+c \equiv b+d \pmod{n}$.

3°) Propriété 3

a, b, c sont 3 entiers relatifs.

Si $a \equiv b \pmod{n}$, alors $a \times c \equiv b \times c \pmod{n}$.

Démonstration :

Par hypothèse, on a : $a \equiv b \pmod{n}$ donc $n \mid a-b$.

On a : $a \times c - b \times c = (a-b) \times c$.

Or $n \mid a-b$ donc $n \mid (a-b) \times c$.

D'où $n \mid a \times c - b \times c$.

On en déduit que $a \times c \equiv b \times c \pmod{n}$.

4°) Propriété 4

a, b, c, d sont 4 entiers relatifs.

Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a \times c \equiv b \times d \pmod{n}$.

Démonstration :

Par hypothèse, on a $a \equiv b \pmod{n}$ d'où $a \times c \equiv b \times c \pmod{n}$.
Par hypothèse, on a $c \equiv d \pmod{n}$ d'où $b \times c \equiv b \times d \pmod{n}$.
Par transitivité de la relation de congruence modulo n, on en déduit que $a \times c \equiv b \times d \pmod{n}$.

5°) Propriété 5

a et b sont 2 entiers relatifs.
k est un entier naturel.

Si $a \equiv b \pmod{n}$, alors $a^k \equiv b^k \pmod{n}$.

Démonstration :

On écrit : $a \equiv b \pmod{n}$
$a \equiv b \pmod{n}$
k fois
……..
$a \equiv b \pmod{n}$

On multiplie ces congruences membre à membre.

On obtient : $\underbrace{a \times a \times \ldots \times a}_{k \text{ facteurs}} \equiv \underbrace{b \times b \times \ldots \times b}_{k \text{ facteurs}}$.

On en déduit : $a^k \equiv b^k \pmod{n}$.

6°) Propriété 6

x et b sont 2 entiers relatifs.
a est un entier naturel non nul qui divise x.

$$\frac{x}{a} \equiv b \pmod{n} \Leftrightarrow x \equiv ab \pmod{na}$$

IV. Commentaires sur les propriétés

1°) Propriétés de réflexivité, symétrie et transitivité

On dit que la relation de congruence modulo n est une **« relation d'équivalence »**.

2°) Compatibilité

• Les propriétés du 1°) et du 2°) sont appelées propriétés de **compatibilité** de la relation de congruence modulo n **avec l'addition**.

• Les propriétés du 3°) et du 4°) sont appelées propriétés de **compatibilité** de la relation de congruence modulo n **avec la multiplication**.

• Attention, la relation de congruence modulo n n'est pas compatible avec la division.

• Attention, on ne peut pas passer à la racine carrée dans une congruence.

V. Congruences et division euclidienne

1°) Propriété 1

a est un entier relatif.
n est un entier naturel supérieur ou égal à 2.

$a \equiv 0 \pmod{n}$ si et seulement si a est divisible par n.

Démonstration (évidente) :

$a \equiv 0 \pmod{n} \Leftrightarrow a - 0 = a$ est divisible par n

2°) Propriété 2

Tout entier relatif a est congru modulo n à son reste dans la division euclidienne par n.

Démonstration (évidente)

3°) Propriété 3

a et b sont deux entiers relatifs.
n est un entier naturel supérieur ou égal à 2.

$a \equiv b \pmod{n}$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Démonstration :

On doit raisonner dans les deux sens.

• Supposons que $a \equiv b \pmod{n}$.

On a alors $n \mid a - b$.

On note q et r respectivement le quotient et le reste de la division euclidienne de a par n.
On note q' et r' respectivement le quotient et le reste de la division euclidienne de b par n.

On a alors :
$a = nq + r$ et $0 \leqslant r < n$;
$b = nq' + r'$ et $0 \leqslant r' < n$.

Or $n \mid a - b$ donc il existe un entier k tel que $a - b = kn$.

Par suite, $a = b + kn$.

On a donc $a = (nq' + r') + kn$.

D'où : $a = nq' + kn + r'$

$$a = n(q' + k) + r'$$

Comme $0 \leqslant r' < n$, on en déduit que r' est le reste de la division euclidienne de a par n.
D'où $r = r'$.

• Supposons que a et b ont le même reste dans la division euclidienne par n.

On note r le reste commun aux divisions euclidiennes.
On note q le quotient de la division euclidienne de a par n et q' le quotient de la division euclidienne de b par n.
On a alors $a = nq + r$, $b = nq' + r$ et $0 \leqslant r < n$.

Donc $a - b = (nq + r) - (nq' + r) = n(q - q')$.

On en déduit que $a - b$ est divisible par n.

4°) Conséquences

Les congruences permettent de :
- déterminer si un nombre est divisible par un entier (propriété 1) ;
- déterminer des restes de divisions euclidiennes sans faire de division euclidienne (propriété 2 ou propriété ci-dessous).

a est un entier relatif.
n est un entier naturel supérieur ou égal à 2.

$a \equiv r$ (mod. n) et $0 \leqslant r < n$ signifie que r est le reste de la division euclidienne de a par n.

Voir exercices.

5°) Corollaire utile en pratique

a et b sont 2 entiers relatifs tels que $a \equiv b$ (mod. n).
n est un entier naturel supérieur ou égal à 2.

Dans ce cas, a est divisible par n si et seulement si b est divisible par n.

VI. Critères de divisibilité

1°) Propriétés

On se réfère aux chiffres qui composent l'écriture en base dix.

• Un entier est divisible par 2 si et seulement si il se termine par un chiffre pair (0, 2, 4, 6 ou 8).

• Un entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

• Un entier est divisible par 4 si et seulement si le nombre formé par ses deux derniers chiffres (celui des dizaines et celui des unités) est divisible par 4.

• Un entier est divisible par 5 si et seulement si il se termine par 0 ou 5.

• Un entier est divisible par 6 si et seulement si il est divisible à la fois par 2 et par 3.

• Un entier est divisible par 9 si et seulement si la somme des chiffres qui composent son écriture est divisible par 9.

• Un entier est divisible par 10 si et seulement si il se termine par un 0.

• Un entier est divisible par 25 si et seulement si le nombre formé par ses deux derniers chiffres est divisible par 25.

On peut prendre un exemple, par exemple 248 pour mieux comprendre.

Soit n un entier naturel.

• Un entier naturel est divisible par 2^n si et seulement si ses n derniers chiffres forment un nombre divisible par 2^n.

• Un entier naturel est divisible par 5^n si et seulement si ses n derniers chiffres forment un nombre divisible par 5^n.

2°) Exemples d'utilisation

Le nombre 47 103 est divisible par 3 (car la somme des chiffres est divisible par 3).

Le nombre 27 424 est divisible par 4 (car le nombre formé par les deux derniers chiffres est divisible par 4).

3°) Démonstrations

On va faire les démonstrations dans le cas des entiers naturels. Le cas des entiers négatifs en découle directement.

Il s'agit d'une application très importante de la notion de congruence.

• Démonstration du critère de divisibilité par 3 pour les entiers naturels

Lemme (à connaître par cœur et à savoir redémontrer) :

Tout entier naturel est congru modulo 3 à la somme de ses chiffres de son écriture en base dix.

On va utiliser les congruences (congruence modulo 3).

On considère un entier naturel N.

On pose $N = \overline{a_n a_{n-1} \ldots a_1 a_0}$ (écriture en base dix).

On a donc $N = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10^2 a_2 + 10 a_1 + a_0$ (décomposition en base dix du nombre N).

Or $10 \equiv 1$ (mod. 3).
Donc pour tout entier naturel k, on a : $10^k \equiv 1$ (mod. 3).

$a_0 \equiv a_0$ (mod. 3)

$10a_1 \equiv a_1$ (mod. 3)

$10^2 a_2 \equiv a_2$ (mod. 3)

⋮

$10^n a_n \equiv a_n$ (mod. 3)

En additionnant membre à membre, on obtient $N \equiv \underbrace{a_n + a_{n-1} + ... + a_2 + a_1 + a_0}$ (mod. 3)

somme des chiffres de l'écriture en base dix de N

[on remplace chaque puissance de 10 par 1 quand on passe en congruence].

On en déduit que N est congru modulo 3 à la somme de ses chiffres de son écriture en base dix.

Application :

N est divisible par 3 si et seulement si $a_n + a_{n-1} + ... + a_2 + a_1 + a_0$ est divisible par 3.

Commentaire :

On peut démontrer ce critère sans utiliser les congruences mais la démonstration utilisant les congruences est de loin la plus efficace et la plus rapide.
Dans son *Traité du Triangle arithmétique* de 1654, Pascal a été le premier, comme il le dit lui-même, à démontrer ce critère de divisibilité.

Généralisation du lemme :

Tout entier naturel est congru à la somme de ses chiffres en base *b* (*b* entier naturel supérieur ou égal à 2) modulo $b-1$.

• Démonstration du critère de divisibilité par 9

Même principe que pour la divisibilité par 3 (on raisonne en congruence modulo 9).

• Démonstration du critère de divisibilité par 4

Lemme (à connaître par cœur et à savoir redémontrer) :

Tout entier naturel est congru modulo 4 au nombre formé par ses deux derniers chiffres en base dix.

On considère un entier naturel N.

On pose $N = \overline{a_n a_{n-1} ... a_1 a_0}$ (écriture en base 10).
On suppose que $n \geqslant 2$.

On a donc $N = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$ (décomposition en base 10 du nombre N).

Or $10^2 \equiv 0$ (mod. 4).
Donc pour tout entier $p \geqslant 2$, on a : $10^p = 10^{p-2} \times 10^2$ (avec $p-2 \geqslant 0$) d'où $10^p \equiv 0$ (mod. 4).

Par conséquent, $N \equiv 10a_1 + a_0$ (mod. 4).

$10a_1 + a_0$ n'est autre que l'entier noté $\overline{a_1 a_0}$.

D'où N est divisible par 4 si et seulement si $\overline{a_1 a_0}$ est divisible par 4.

• Démonstration des autres critères de divisibilité

Même principe.

• Il existe d'autres critères de divisibilité qui seront étudiés en exercice.

Les lemmes doivent être sus par cœur. Outre les critères de divisibilité qu'ils permettent de démontrer, ils permettent aussi de déterminer mentalement des restes de division euclidienne (par 3, 9, 4 etc.).

3°) La preuve par 9

VII. Application pratique des congruences aux clefs de contrôle

On utilise fréquemment des codages dans différentes situations : N°INSEE (c'est-à-dire numéro de sécurité sociale), code ISBN pour les publications, codes barres.

Ces codes sont composés d'un matricule (grand nombre formé selon certains critères) et d'une clef.

MATRICULE (grand nombre)	CLEF (petit nombre)

Ces clefs sont calculées à partir du reste de division euclidienne du matricule selon un procédé propre à chaque type de code.

Comme le matricule est un grand nombre et que seul le reste est intéressant, on utilise les congruences sans faire la division euclidienne.

La clef de contrôle sert à détecter d'éventuelles erreurs de saisie du matricule (telles que l'inversion de deux chiffres).

VIII. Quelques mots sur la cryptographie

1°) Qu'est-ce que la cryptographie ?

Le mot cryptographie est formé de deux racines grecques à connaître :

kruptos = caché
graphein = écriture
} Messages codés

Il s'agit de l'étude des messages codés.

L'utilisation de messages codés remonte à l'Antiquité (Jules César et même avant).

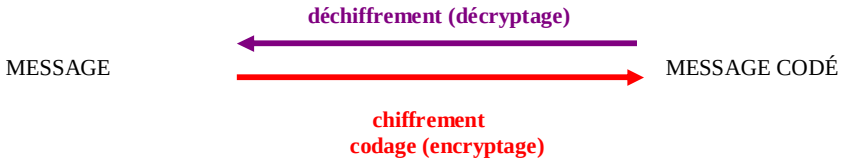
La cryptographie est très utilisée encore aujourd'hui dans de nombreux domaines (domaine militaire, industriel, bancaire).

Exemples :

- codes secrets à 4 chiffres de cartes bancaires ;
- décodeur pour regarder des chaînes cryptées (par exemple, Canal +)
- cartes vitales

La cryptographie utilise les mathématiques et plus précisément l'arithmétique d'où la recherche active dans ce domaine.

2°) Principe



Les techniques anciennes de cryptographie étaient assez simples.
Aujourd'hui, on cherche des techniques très compliquées.

3°) Méthode de Jules César (environ 50 avant Jésus-Christ)

• Principe :

On remplace une lettre par celle située trois rangs plus loin de l'alphabet.

A → D, B → E, Y → B, Z → C etc.

• Modélisation (chiffrage) :

A ↔ 1

B ↔ 2

…

Z ↔ 26

La règle du code de César consiste à ajouter 3 modulo 26.

X ↔ 24

$24+3=27$

$27 \equiv 1 \pmod{26}$

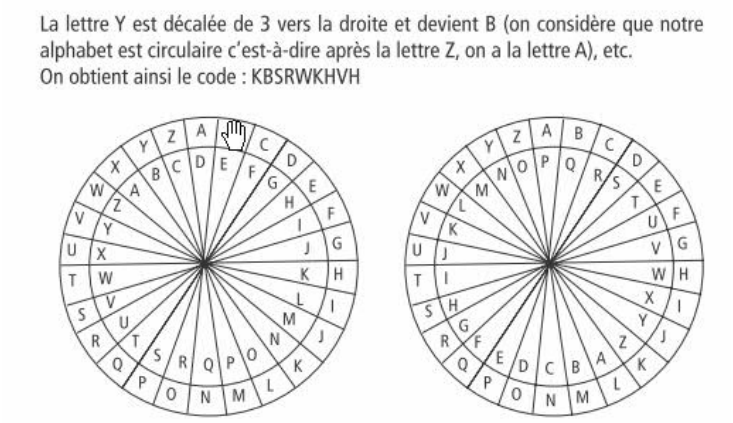
Donc X → A.

• Exemple :

« PROLHUH VHMRXUQD D SHCHQDY » → « MOLIERE SÉJOURNA À PEZENAS »

• Faiblesse : très simple

TS spé Sequence-01 Très bon cours codage de Jules César avec roue de codage etc..pdf



4°) Code Enigma

« Je vais prendre mon parapluie »

On décide d'une clé.

Exemple : A M I
1 ; 13 ; 9

On ajoute 1 à la 1ère lettre, 13 à la 2e lettre, 9 à la 3e lettre
Et on recommence…

Un film sur le sujet :

« Imitation Game » ou Le Jeu de l'imitation au Québec (The Imitation Game) est un film américano-britannique réalisé par Morten Tyldum, sorti en 2014.
Le film est inspiré de la vie du mathématicien et cryptanalyste britannique Alan Turing, notamment pendant la Seconde Guerre mondiale où il a travaillé à Bletchey Park.
Le titre du film est une référence à l'introduction de l'article écrit par Alan Turing en 1950 pour présenter ses recherches sur l'intelligence artificielle et notamment ce qui est devenu par la suite le test de Turing. Celui-ci est brièvement évoqué dans le film, mais n'est pas le sujet principal du film, qui se concentre sur son travail sur Enigma.

On dit que le décryptage du code Enigma a permis de gagner plusieurs années pendant la Seconde Guerre Mondiale.

5°) Algorithmes de codages et de décodages

Codage affine (ou chiffrement affine) : deux lettres différentes doivent être codées par deux chiffres différents.

Le texte doit d'abord être numérisé (étape de numérisation).

IX. Inverse d'un nombre modulo *n*

Dans tout le paragraphe, *n* est un entier naturel fixé supérieur ou égal à 2.

1°) Définition

Soit *n* un entier naturel fixé supérieur ou égal à 2.
Soit *a* un entier relatif.

On dit que *a* admet un inverse modulo *n* (pour le produit) s'il existe un entier relatif *x* tel que $ax \equiv 1 \ [n]$.

On dit que *x* est un inverse de *a* modulo *n*.

2°) Commentaires

Il faut bien comprendre qu'on ne peut pas écrire $\frac{1}{a}$ car $\frac{1}{a}$ est un nombre rationnel non entier dès lors que *a* est différent de 1 et de – 1.

Il n'y a pas de notation particulière d'inverse pour les congruences.

3°) Problèmes

Tout entier admet-il un inverse modulo *n* ? Comment caractériser ceux qui en ont un ?

La réponse est non pour la première question. De manière évidente, 0 n'a pas d'inverse modulo *n*.

4°) Exemple

Déterminer un inverse de 2 modulo 9.

Il faut trouver un entier *x* tel que $2x \equiv 1 \pmod 9$.

Il n'y a pour l'instant pas d'autre méthode que de chercher à la main en testant des entiers.

On commence à 0 par commodité.

$2 \times 0 = 0$ qui n'est pas congru à 1 modulo 9.
$2 \times 1 = 2$ qui n'est pas congru à 1 modulo 9.
$2 \times 3 = 6$ qui n'est pas congru à 1 modulo 9.
$2 \times 4 = 8$ qui n'est pas congru à 1 modulo 9.
$2 \times 5 = 10$ qui est congru à 1 modulo 9.

On a $2 \times 5 \equiv 1 \pmod 9$ donc 5 est un inverse de 2 modulo 9.

5°) Propriété

Supposons que *a* admettent deux inverses *b* et *c* modulo *n*.
Alors $b \equiv c \pmod n$.

Démonstration :

Par hypothèse, on a $a \times b \equiv 1 \pmod n$ et $a \times c \equiv 1 \pmod n$.

En multipliant les deux membres de la première congruence par *c*, on obtient $abc \equiv c \pmod n$.

En multipliant les deux membres de la deuxième congruence par *b*, on obtient $abc \equiv b \pmod n$.

Par transitivité de la relation de congruence, on obtient $b \equiv c \pmod n$.

6°) Propriété (critère pour qu'un entier relatif admette un inverse modulo *n*)

a admet un inverse modulo *n* ⇔ *a* est premier avec *n*.

Démonstration :

1er sens : On suppose que *a* admet un inverse modulo *n*.
Il existe donc un entier relatif a' tel que $aa' \equiv 1 \pmod n$.
Cette relation permet de dire qu'il existe un entier relatif *k* tel que $aa' = 1 + kn$ soit $aa' - kn = 1$.
On en déduit que *a* et *n* sont premiers entre eux puisque l'on a obtenu une combinaison linéaire à coefficients entiers relatifs égale 1.

2e sens : On suppose que *a* et *n* sont premiers entre eux.
D'après le théorème de Bezout qui sera vu plus tard dans le chapitre sur PGCD et PPCM, il existe deux entiers relatifs *u* et *v* tels que $au + nv = 1$ ce qui donne $au \equiv 1 \pmod n$. *a* admet donc *u* pour inverse modulo *n*.

7°) Méthodes pour trouver un inverse modulo *n*

• Méthode 1 : à la main, en testant différentes valeurs
Cette méthode marche si c'est simple, sinon c'est long.

• Méthode 2 : à la calculatrice, en rentrant la fonction $f : x \mapsto$ reste de la division euclidienne de *ax* par *n*
On regarde dans la table des valeurs.

• Méthode 3 : à l'aide d'un programme Python, une boucle « Pour »

• Méthode 4 : à l'aide de l'identité de Bezout
On utilise le 2e sens de la démonstration du critère pour qu'un entier admet un inverse modulo *n*.

8°) Équivalence fondamentale

Propriété :

Soit *a* un entier relatif.
On suppose que *a* et *n* sont premiers entre eux.
On note *b* un inverse de *a* modulo *n*.

On a l'équivalence suivante pour *x* et *y* entiers relatifs quelconques :
$ax \equiv y \pmod n \Leftrightarrow x \equiv by \pmod n$

Démonstration :

On sait que $a \times b \equiv 1 \pmod{n}$.

On raisonne en deux temps.

On démontre que si $ax \equiv y \pmod{n}$, alors $x \equiv by \pmod{n}$.
On démontre que si $x \equiv by \pmod{n}$, alors $ax \equiv y \pmod{n}$.

1ère partie :

On suppose que $ax \equiv y \pmod{n}$.

On multiplie les deux membres de cette congruence par b.

On obtient $abx \equiv by \pmod{n}$.

On utilise ensuite la congruence a $a \times b \equiv 1 \pmod{n}$.
On multiplie les deux membres de cette congruence par x.
On obtient $abx \equiv x \pmod{n}$.

Par transitivité de la relation de congruence, on obtient : $x \equiv by \pmod{n}$.

2e partie : idem

9°) Application à la résolution des équations $ax \equiv b \pmod{n}$ où a et b sont des entiers relatifs

Exemple :

Résoudre dans $\mathbb{Z}$ l'équation $2x \equiv 3 \ [9] \ (1)$.

On commence par chercher un inverse de 2 modulo 9.
On trouve aisément que 5 est un inverse de 2 modulo 9 car $2 \times 5 \equiv 1 \pmod{9}$ (exemple du 4°) donc on peut l'appliquer la propriété d'équivalence fondamentale.

$$(1) \Leftrightarrow x \equiv 5 \times 3 \ [9]$$
$$\Leftrightarrow x \equiv 15 \ [9]$$
$$\Leftrightarrow x \equiv 6 \ [9]$$

On conclut de la manière suivante (très simple) :

Les solutions de l'équation sont tous les entiers relatifs congrus à 6 modulo 9.

Le 8-1-2024

Cours sur les congruences

On a quelques équivalences.

$a \equiv b \ [n] \Leftrightarrow a + k \equiv b + k \ [n]$

$a \equiv b \ [n] \Leftrightarrow -a \equiv -b \ [n]$

Attention cependant à l'implication :

$a \equiv b \ [n] \Rightarrow ka \equiv kb \ [n]$

Lire les articles suivants sur Wikipedia :

- sur François Viète

- sur Antoine et Bonaventure Rossignol (Le Cabinet Noir, le Grand Chiffre)

- lettres de Marie-Antoinette

Compléments sur la cryptographie :

- Exposé par Vincent Davoust en novembre 2011 : le code ASCII

C'est le code ASCII qui permet de passer de l'alphabet « humain » à un alphabet en binaire

- Lecture complémentaire : Lettres codées de Marie-Antoinette décryptées par Jacques Patarin

- Trouver des moyens de coder des messages : MPS Fait par Gérald Alletru durant l »année scolaire 2010-2011

- Site d'Alain Pichereau : Une page sur la cryptographique affine et possibilité de coder un petit texte en ligne.

- Nicolas Serey : « Le cryptage de plus de 130 caractères est considéré comme une arme de guerre ».

Le 21 octobre 2011, nous somme allé voir l'article « Cryptographie » du site Wikipedia.

Texte extrait du livre Odyssée TS spécialité page 52

Les plus anciennes techniques de chiffrement remontent au Ve siècle avant Jésus-Christ avec les Hébreux qui intervertissaient les lettres (le A par le Z, le B par le Y…). Mais c'est à l'époque romaine sous Jules César, que se développa le chiffrement par décalage. Le principe, assez simple, consistant à décaler toutes les lettres du même nombre de pas (si A devient E, B devient F, etc.) Cette méthode simple et facile à décrypter perdura longtemps, notamment de part la faible alphabétisation des populations. Elle fut encore utilisée lors de la guerre de Sécession par les sudistes et aussi par les Russes pendant la Première guerre mondiale.