Cours : Divisibilité dans $\mathbb{Z}$

A Congruences modulo n dans $\mathbb{Z}$, avec n entier naturel non nul

❶ Exemples

Considérons les entiers relatifs :

–13 , –8 , 7 et 8 ; effectuons leurs différences deux à deux et observons si cette différence est multiple de 5.

$(-13)-(-8) = -5$	:	c'est un multiple de 5	(1)
$(-13)-7 = -20$	:	c'est un multiple de 5	(2)
$(-13)-8 = -21$	:	ce n'est pas un multiple de 5	(3)
$(-8)-7 = -15$	:	c'est un multiple de 5	(4)
$(-8)-8 = -16$	:	ce n'est pas un multiple de 5	(5)
$7-8 = -1$	:	ce n'est pas un multiple de 5	(6)

Dans les lignes (1), (2) et (4) la différence est un multiple de 5 nous dirons que :

–13 et –8		sont « congrus » modulo 5
–13 et 7		sont « congrus » modulo 5
–8 et 7		sont « congrus » modulo 5

et nous écrirons :

$-13 \equiv -8$	(mod 5)	ou encore	$-13 \equiv -8$	[5]	ou encore	$-13 \equiv -8$	(5)
$-13 \equiv 7$	(mod 5)	ou encore	$-13 \equiv 7$	[5]	ou encore	$-13 \equiv 7$	(5)
$-8 \equiv 7$	(mod 5)	ou encore	$-8 \equiv 7$	[5]	ou encore	$-8 \equiv 7$	(5)

mais le cas de la ligne (3), par exemple, se traduit par (-13) n'est pas « congru » à 8 modulo 5 et peut s'écrire :

$$-13 \not\equiv 8 \quad [5]$$

La signe utilisé ressemble au signe « égal » : = , mais ici, il y a trois barres superposées.

❷ Définition et notation

Soit n un entier naturel non nul donné, et soient x et y deux entiers relatifs quelconques.

On dit que x est congru à y modulo n si la différence $x-y$ est un multiple de n.

Dans ce cas on note :

$x \equiv y$ (mod n) ou encore $x \equiv y$ [n] ou encore $x \equiv y$ (n)

et on lit « x congru à y modulo n ».

Remarque *si* $x-y$ *est multiple de n, on a aussi* $y-x$ *multiple de n*

donc si : $x \equiv y\ [n]$ *on a aussi :* $y \equiv x\ [n]$

Cours : Divisibilité dans $\mathbb{Z}$

B Propriétés de compatibilité

❶ Addition, soustraction et multiplication

Propriété ❶ : Addition et soustraction de congruences de même module

La relation de congruence modulo n est compatible avec l'addition et avec la soustraction dans $\mathbb{Z}$; c'est-à-dire que si on a : $x \equiv y\ [n]$ et $x' \equiv y'\ [n]$

alors on a aussi : $x + x' \equiv y + y'\ [n]$

et : $x - x' \equiv y - y'\ [n]$

Cela veut dire *que si on a deux congruences modulo n, on peut les* ***ajouter*** *membre à membre ou les* ***retrancher*** *membre à membre et on obtient encore une congruence modulo n.*

Démonstration

$x \equiv y\ [n]$ se traduit par $x - y$ multiple de n

$x' \equiv y'\ [n]$ se traduit par $x' - y'$ multiple de n

On en déduit que la « somme » $(x - y) + (x' - y')$ est encore un multiple de n, c'est-à-dire :

$(x + x') - (y + y')$ multiple de n ;

ceci veut dire $x + x' \equiv y + y'\ [n]$.

En remplaçant le mot « somme » par le mot « différence » dans le raisonnement précédent, on prouve : $x - x' \equiv y - y'\ [n]$

Exemple

On sait $\begin{cases} -13 \equiv -8 & [5] \\ 7 \equiv -8 & [5] \end{cases}$

En ajoutant membre à membre on obtient : $-6 \equiv -16$ [5]

En retranchant membre à membre on obtient : $-20 \equiv 0$ [5]

(on peut contrôler les deux nouvelles congruences obtenues en revenant à la définition).

Propriété ❷ : Multiplication de congruences de même module

La relation de congruence modulo n est compatible avec la multiplication dans $\mathbb{Z}$; c'est-à-dire que

si on a : $x \equiv y\ [n]$ et $x' \equiv y'\ [n]$

alors on a aussi : $xx' \equiv yy'\ [n]$

Cela veut dire *que si on a deux congruences modulo n, on peut les* ***multiplier*** *membre à membre et on obtient encore une congruence modulo n.*

Démonstration

$x \equiv y\ [n]$ donc il existe k de $\mathbb{Z}$ tel que $x - y = kn$

d'où $x = y + kn$

$x' \equiv y'\ [n]$ donc il existe k' de $\mathbb{Z}$ tel que $x' - y' = k'n$

d'où $x' = y' + k'n$

Cours : Divisibilité dans $\mathbb{Z}$

On a donc : $xx' = (y+kn)(y'+k'n) = yy' + n(ky' + k'y + kk'n)$

Posons $k'' = ky' + k'y + kk'n$; k'' est un élément de $\mathbb{Z}$ et $xx' - yy' = k''n$.

Cette dernière ligne prouve : $xx' \equiv yy'\ [n]$.

Exemple

On sait $\begin{cases} -13 \equiv -8 & [5] \\ 7 \equiv -8 & [5] \end{cases}$

on en déduit : $-13 \times 7 \equiv (-8)\times(-8)$ [5] c'est-à-dire : $-91 \equiv 64$ [5]

(on peut encore contrôler ce résultat en revenant à la définition).

Propriété ❸ : Multiplication par un entier

Si $x \equiv y\ [n]$ alors quel que soit k de Å

on a aussi : $kx \equiv ky\ [n]$

Démonstration

Cette propriété est un cas particulier de la propriété 2, car : $x \equiv y\ [n]$ et $k \equiv k\ [n]$.

Exemple

On sait $-13 \equiv -8$ [5]

En multipliant les deux membres par le même nombre (-3) (par exemple)

on obtient : $39 \equiv 24$ [5]

Propriété ❹ : Elévation à une puissance

Si $x \equiv y\ [n]$ alors quel que soit l'entier naturel p

on a aussi : $x^p \equiv y^p\ [n]$

Cette propriété est une conséquence de la propriété 2; on l'établit en faisant un raisonnement par récurrence).

Exemple

On sait $7 \equiv 2$ [5]

Donc $7^2 \equiv 2^2$ [5] c'est à dire $7^2 \equiv 4$ [5] ou encore $7^2 \equiv -1$ [5]

De même $7^3 \equiv 2^3$ [5] c'est à dire $7^3 \equiv 8$ [5] ou encore $7^3 \equiv 3$ [5]

De même $7^4 \equiv 2^4$ [5] c'est à dire $7^4 \equiv 16$ [5] ou encore $7^4 \equiv 1$ [5]

Pour cette dernière ligne, on peut aussi procéder de la façon suivante :

puisque $7^2 \equiv -1$ [5] on en déduit $(7^2)^2 \equiv (-1)^2$ [5] c'est à dire $7^4 \equiv 1$ [5]

Remarque

Cette dernière idée est importante : quand un nombre est congru à –1 modulo n, le carré de ce nombre est congru à 1 modulo n.

❷ Prudence avec la division d'une congruence par un entier

Exemple : on sait $18 \equiv 10$ [8]

• En divisant les deux membres par 2, a-t-on encore une congruence modulo 8 ?

réponse : non car $9 \not\equiv 5$ [8]

Cours : Divisibilité dans $\mathbb{Z}$

Remarque *Cela veut dire qu'en général « $x \equiv y$ [n] » n'implique pas « $\frac{x}{k} = \frac{y}{k}$ [n] »*

- Par contre : $9 \equiv 5$ [4] (on a divisé aussi le module par 2).

Propriété ❺ : Simplification d'une congruence

Soient x et y deux entiers divisibles par un même entier naturel k ;

❶ si ($x \equiv y$ [n] et n divisible par k) alors $\frac{x}{k} \equiv \frac{y}{k}$ $\left[\frac{n}{k}\right]$ (on divise aussi le module)

❷ si ($x \equiv y$ [n] et n et k premiers entre eux) alors $\frac{x}{k} \equiv \frac{y}{k}$ [n]

Démonstration

❶ Puisque x, y et n sont divisibles par k, il existe des entiers x', y' et n' tels que $x = kx'$, $y = ky'$ et $n = kn'$.

La congruence $x \equiv y$ [n] se traduit par l'existence d'un entier p tel que $x - y = p \times n$, donc $kx' - ky' = p(kn')$; en simplifiant par k, on obtient : $x' - y' = pn'$; la différence $x' - y'$ étant un multiple de n', cela se traduit par : $x' = y'$ [n'] ou encore : $\frac{x}{k} \equiv \frac{y}{k}$ $\left[\frac{n}{k}\right]$.

❷ De même, puisque x et y sont divisibles par k, il existe des entiers x' et y' tels que $x = kx'$ et $y = ky'$.

Avoir $x \equiv y$ [n] veut dire que n divise $x - y$, c'est à dire n divise $kx' - ky'$ ou encore n divise $k(x' - y')$.

On sait ici que n et k sont premiers entre eux; d'après le théorème de Gauss, on en déduit que n divise $x' - y'$; cela se traduit par la congruence : $x' \equiv y'$ [n], ou encore $\frac{x}{k} \equiv \frac{y}{k}$ [n].

Exemples

- On a $18 \equiv 10$ [8] ; on peut diviser 18, 10 et aussi le module 8 par 2 et on a bien : $9 \equiv 5$ [4] (il faut bien remarquer qu'on a aussi divisé le module par 2).
- On a $36 \equiv 6$ [5] ; 36 et 6 sont divisibles par 3 et ce diviseur 3 est premier avec le module 5; on constate que l'on a bien : $12 \equiv 2$ [5] et de même puisque 2 est premier avec 5, on a aussi $6 \equiv 1$ [5].

Cours : Divisibilité dans $\mathbb{Z}$

C Division euclidienne d'un entier relatif a (a dans $\mathbb{Z}$) par un entier naturel b non nul (b dans $\mathbb{N}^*$)

*** Le cas $a \geqslant 0$** (a dans $\mathbb{N}$) a déjà été traité dans la première séquence ; il s'agit de la division euclidienne d'un entier **naturel** a par un **entier naturel b non nul**.

Il existe un quotient q unique et un reste r unique dans $\mathbb{N}$ tels que :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b$$

*** Cas $a < 0$**

Exemple

on veut diviser (-20) par 3 :

on sait $20 = 3 \times 6 + 2$

donc $-20 = 3 \times (-6) - 2$
$= 3 \times (-6) - 3 + 3 - 2$
$= 3 \times (-7) + 1$

On retient la dernière écriture car on a le reste 1 dans $\mathbb{N}$ et inférieur strictement à 3.

Le cas général se traite comme l'exemple précédent pour lequel on observe :

$20 = \mathbf{3} \times 6 + \mathbf{2}$ **et** $0 \leqslant 2 < 3$

$-20 = \mathbf{3} \times (-7) + \mathbf{1}$ et $0 \leqslant 1 < 3$

Le quotient de la division euclidienne de (-20) par 3 est (-7) et le reste est 1.

Autres exemples

▶ *division euclidienne de (-503) par 26*

On a : $503 = 26 \times 19 + 9$ **et** $0 \leqslant 9 < 26$

$-503 = 26 \times (-19) - 9$
$= 26 \times (-20) + 26 - 9$
$= 26 \times (-20) + 17$ **et** $0 \leqslant 17 < 26$

Le quotient de la division euclidienne de (-503) par 26 est $q = -20$ et le reste est $r = 17$.

▶ *division euclidienne de (-1036) par 4.*

On a : $1036 = 4 \times 259$ (reste nul car 1036 est multiple de 4)

donc : $-1036 = 4 \times (-259)$

Le quotient de la division euclidienne de (-1036) par 4 est (-259) est le reste est $r = 0$.

Propriété 6

Quel que soit l'**entier relatif a** (a dans $\mathbb{Z}$) et l'**entier naturel non nul b** (b dans $\mathbb{N}^*$), il existe un unique nombre q dans $\mathbb{Z}$, et un unique nombre r dans $\mathbb{N}$ vérifiant :

$$a = bq + r \quad \textbf{et} \quad 0 \leqslant r < b .$$

q s'appelle le quotient et r s'appelle le reste de la division euclidienne de a par b.

Remarque

Cette propriété généralise la division euclidienne vue sur les entiers naturels, et permet d'avoir toujours la même condition sur le reste :

$$0 \leqslant \text{reste} < \text{diviseur}$$

Cours : Divisibilité dans $\mathbb{Z}$

D Lien entre division euclidienne par n ($n \in \mathbb{N}^*$) et congruente modulo n

Soit a dans $\mathbb{Z}$ et n dans $\mathbb{N}^*$.

La division euclidienne de a par n se traduit par : $a = nq + r$ **et** $0 \leq r < n$

donc $a - r = nq$ donc $a - r$ multiple de n,

donc $a \equiv r\ [n]$.

Ce résultat qui aura des applications importantes, fait l'objet de la propriété suivante :

Propriété 7

1. un entier relatif a est congru modulo n à son reste r dans la division euclidienne de a par n
2. $x \equiv y \pmod{n} \Leftrightarrow$ x et y ont même reste dans la division euclidienne par n.

E Quelques exemples

Exemple 1 Quel est le reste dans la division euclidienne de 2006^{503} par 7 ?

(Il ne s'agit bien sûr pas de calculer ce nombre 2006^{503}).

Réponse

La division euclidienne de 2006 par 7 donne : $2006 = 7 \times 286 + 4$

Le reste est 4 donc $2006 \equiv 4 \pmod 7$

La compatibilité de la relation de congruence avec l'élévation à une puissance permet de dire que : pour tout exposant n de $\mathbb{N}^*$ on aura aussi $2006^n \equiv 4^n \pmod 7$ et en particulier $2006^{503} = 4^{503} \pmod 7$.

Il va être beaucoup plus simple d'examiner les puissances successives de 4 :

on a :	$4 \equiv 4$	(mod 7)	
$4^2 \equiv 16$ donc :	$4^2 \equiv 2$	(mod 7)	car $16 = 7 \times 2 + 2$
d'où :	$4^3 \equiv 4 \times 2$	(mod 7)	(en multipliant les 2 membres par 4)
c'est-à-dire :	$4^3 \equiv 8$	(mod 7)	
ou encore :	$4^3 \equiv 1$	(mod 7)	car $8 = 7 \times 1 + 1$

Ce dernier résultat est très important, car il va simplifier beaucoup les choses du fait que :

$(4^3)^2 \equiv 1^2 \equiv 1 \pmod 7$

$(4^3)^3 \equiv 1^3 \equiv 1 \pmod 7$

$(4^3)^4 \equiv 1^4 \equiv 1 \pmod 7$

$\vdots$

$(4^3)^k \equiv 1^k \equiv 1 \pmod 7$ pour k quelconque de $\mathbb{N}^*$

Cours : Divisibilité dans $\mathbb{Z}$

Ne perdons pas de vue que : $2006^{503} \equiv 4^{503} \pmod 7$

Effectuons la division euclidienne de 503 par 3. $503 = 3 \times 167 + 2$

Donc $4^{503} = 4^{(3\times 167+2)} = (4^3)^{167} \times 4^2$

D'après les calculs faits avant on a :

$(4^3)^{167} \equiv 1^{167} \equiv 1 \pmod 7$

et $4^2 \equiv 2 \pmod 7$

donc $(4^3)^{167} \times 4^2 \equiv 2 \pmod 7$

c'est-à-dire $4^{503} \equiv 2 \pmod 7$ ou encore

$2006^{503} \equiv 2 \pmod 7$

2 étant tel que : $0 \leqslant 2 < 7$, est le reste dans la division euclidienne de 2006^{503} par 7.

Remarque *La méthode mise en œuvre dans cet exemple est **très importante**.*

Exemple 2 Calculer le reste dans la division euclidienne par 7 du nombre : $19^{52} \times 23^{41}$

Réponse

▶ $19 \equiv 5\ [7]$ d'où $19^{52} \equiv 5^{52}\ [7]$

Intéressons-nous aux puissances successives de 5.

$5^2 \equiv 4 \ [7]$

$5^3 \equiv 6 \ [7]$

$\equiv -1 \ [7]$

donc $(5^3)^2 \equiv (-1)^2 \ [7]$

c'est-à-dire $5^6 \equiv 1 \ [7]$

d'où pour tout k de $\mathbb{N}^*$ on aura $5^{6k} \equiv 1 \ [7]$ car $1^k = 1$

Effectuons la division euclidienne de 52 par 6 : $52 = 6 \times 8 + 4$

donc $5^{52} = 5^{6\times 8+4} = 5^{6\times 8} \times 5^4$

or $5^{6\times 8} \equiv 1 \ [7]$ et $5^4 \equiv 2 \ [7]$

d'où en multipliant membre à membre, on obtient : $5^{52} \equiv 2 \ [7]$

Il en résulte : $19^{52} \equiv 2 \ [7]$.

▶ Effectuons un travail analogue pour 23^{41} .

Cours : Divisibilité dans $\mathbb{Z}$

$23 \equiv 2 \quad [7] \quad$ donc $\quad 23^{41} \equiv 2^{41} \quad [7]$

$2^2 \equiv 4 \quad [7]$

$2^3 \equiv 8 \equiv 1 \quad [7] \quad$ donc $\quad 2^{3k} \equiv 1 \quad [7]$

$41 = 3 \times 13 + 2$

donc $\quad 2^{41} = 2^{3\times 13+2} = 2^{3\times 13} \times 2^2 \equiv 1 \times 4 \equiv 4 \quad [7]$

Récapitulatif :

$19^{52} \equiv 2 \quad [7] \quad$ et $\quad 23^{41} \equiv 4 \quad [7]$

d'où $\quad 19^{52} \times 23^{41} \equiv 8 \equiv 1 \quad [7]$

Conclusion : le reste de $19^{52} \times 23^{41}$ dans la division euclidienne par 7 est 1.

Remarque

Il est parfois utile de faire apparaître des nombres négatifs asses tôt dans les calculs de congruences ; ici :

$19 \equiv 5$ [7] donc aussi $19 \equiv -2$ [7]

$23 \equiv 2$ [7]

D'où $19^{52} \times 23^{41} \equiv (-2)^{52} \times 2^{41} \equiv 2^{52} \times 2^{41} \equiv 2^{93} \equiv (2^3)^{31}$ [7]

Or $2^3 = 8 \equiv 1$ [7] donc $(2^3)^{31} \equiv 1^{31} \equiv 1$ [7]

Cette méthode évite d'étudier les puissances de 5 modulo 7.

Cours : Divisibilité dans $\mathbb{Z}$

F Le petit théorème de Fermat

Le but de ce paragraphe est de démontrer le théorème suivant :

Si p est un nombre **premier** et a un entier naturel **non divisible par p**, alors $a^{p-1}-1$ est divisible par p, c'est à dire $a^{p-1} \equiv 1 \pmod p$.

Commentaire

Ce théorème est souvent appelé « petit théorème de Fermat », par opposition au « grand théorème de Fermat » dont l'énoncé est : Lorsque n est un entier supérieur ou égal à trois, l'équation $x^n + y^n = z^n$, n'a pas de solutions en nombres entiers, hormis la solution $x = y = z = 0$ ».

Fermat a énoncé ce théorème sans en laisser de démonstration. La preuve en a été faite finalement en 1997, plus de trois cents après, et après que des générations de mathématiciens aient tenté, sans succès, de le démontrer. Mais parmi ceux qui n'ont pas réussi, certains ont « apporté une pierre », et contribué à l'édifice de la solution présentée par le mathématicien anglais Andrew Wiles (1997).

Une démonstration du petit théorème consiste à écrire la liste des multiples de a jusqu'à $(p-1)a$:

$$a, 2a, 3a, \ldots (p-1)a$$

Etape 1 Montrons que deux quelconques de ces p nombres ont des restes *distincts* et *non nuls* dans la division par p.

Pour cela on fait un raisonnement par l'absurde.

▶ Supposons que l'un de ces nombres, par exemple ka pour $1 \leq k \leq p-1$ soit divisible par p.

p étant premier, non diviseur de a, diviserait k ; mais cela est impossible car k est plus petit que p.

Il en résulte qu'aucun des nombres de la liste admet 0 comme reste dans la division par p.

▶ Supposons que deux de ces nombres, par exemple ka et ka′ pour $1 \leq k \leq p-1$ et $1 \leq k' \leq p-1$ ait le même reste dans la division par p. Cela veut dire que $ka \equiv k'a \pmod p$ donc $(k-k')a \equiv 0 \bmod p$ donc p divise $(k-k')a$. Mais p est premier et ne divise pas a, donc p doit diviser $k-k'$ c'est-à-dire $k \equiv k' \pmod p$; ceci est impossible car ces deux nombres k et k′ sont distincts et compris entre 1 et $p-1$.

Conclusion : ces p nombres a, 2a, 3a, …, (p – 1)a admettent p restes distincts non nuls dans la division par p.

A *l'ordre près*, ces restes sont donc 1, 2, 3, …, p – 1.

Etape 2 Montrons que le produit de ces p nombres est congru à $(p-1)!$ dans la congruence modulo p.

Le produit de ces p nombres est congru modulo p, au produit des restes de chacun d'eux dans la division euclidienne par p ; c'est à dire :

$a \times 2a \times 3a \times \ldots \times (p-1)a \equiv 1 \times 2 \times 3 \times \ldots \times (p-1) \pmod p$, c'est-à-dire :

$$a^{p-1} \times (p-1)! \equiv (p-1)! \pmod p .$$

Les deux membres de la congruence sont divisibles par $(p-1)!$.

On pourra diviser les deux membres par $(p-1)!$ et obtenir une congruence vraie modulo p si on prouve que p et $(p-1)!$ sont premiers entre-eux.

Cours : Divisibilité dans $\mathbb{Z}$

On sait que p est premier, et que p ne divise aucun des nombres 1, 2, 3, …, (p – 1) qui lui sont inférieurs; cela prouve que p et $(p-1)$! sont premiers entre eux; et ainsi on a bien :

$a^{p-1} \equiv 1 \pmod{p}$ c'est à dire $a^{p-1} - 1$ divisible par p.

G Prolongement du petit théorème de Fermat

Déduisez du petit théorème de Fermat le résultat suivant :

Si p est un nombre **premier** et a un entier quelconque, alors $a^p \equiv a \pmod{p}$, c'est-à-dire $a^p - a$ divisible par p.

(On ne suppose plus ici *a* non divisible par *p*, seulement $a > 0$).

En effet :

▶ Si a divisible par p on a aussi a^p divisible par p donc on a bien la différence $a^p - a$ divisible par p.

▶ Si a non divisible par p, d'après le petit théorème de Fermat, on a : $a^{p-1} \equiv 1 \pmod{p}$ et en multipliant les deux membres de la congruence par a, on obtient $a^p \equiv a \pmod{p}$, c'est à dire $a^p - a$ divisible par p.

H Exemples

Exemple 1 Sachant que 101 est un nombre premier,

a) Trouver le reste de 2^{100} dans la division par 101.

b) Trouver le reste de 3^{102} dans la division par 101.

Réponse

a) Puisque 101 est premier et ne divise pas 2, le petit théorème de Fermat permet d'affirmer que $2^{100} \equiv 1 \pmod{101}$, donc le reste de la division de 2^{100} par 101 est 1.

b) Puisque 101 est premier et ne divise pas 3, le petit théorème de Fermat permet d'affirmer que $3^{100} \equiv 1 \pmod{101}$; en multipliant les deux membres de la congruence par 3^2 on obtient : $3^{102} \equiv 3^2 \pmod{101}$, donc le reste de la division de 3^{102} par 101 est 9.

Exemple 2 Trouver le reste de 8^{900} dans la division par 29.

Réponse

Le nombre 29 est premier et ne divise pas 8; d'après le petit théorème de Fermat, on peut affirmer que : $8^{28} \equiv 1 \pmod{29}$.

La division euclidienne de 900 par 28 donne : $900 = 28 \times 32 + 4$.

Donc $8^{900} = 8^{(28\times 32)+4} = (8^{28})^{32} \times 8^4$

Or $8^{28} \equiv 1 \pmod{29}$ donc $(8^{28})^{32} \equiv 1^{32} \equiv 1 \pmod{29}$

D'où : $8^{900} \equiv 8^4 \pmod{29}$; $8^2 = 64 \equiv 6 \pmod{29}$

On a : $8^2 = 64 \equiv 6 \pmod{29}$ donc $8^4 \equiv 6^2 \equiv 36 \equiv 7 \pmod{29}$

Il en résulte : $8^{900} \equiv 7 \pmod{29}$, donc le reste de la division de 8^{900} par 29 est 7.

Cours : Divisibilité dans $\mathbb{Z}$

Exemple 3 Prouver que quelque soit l'entier naturel a non nul, $a^{13} - a$ est divisible par 26.

Réponse

▶ D'après le prolongement du petit théorème de Fermat on peut affirmer que $a^{13} \equiv a \pmod{13}$ car 13 est premier ; cela veut dire $a^{13} - a$ divisible par 13.

▶ Si a est pair, a^{13} est pair, donc $a^{13} - a$ est pair d'où $a^{13} - a$ est divisible par 2.

Si a est impair, a^{13} est impair, donc $a^{13} - a$ est pair d'où $a^{13} - a$ est divisible par 2.

Dans tous les cas on a : $a^{13} - a$ divisible par 13 et 2, nombres qui sont premiers entre eux, donc $a^{13} - a$ est divisible par leur produit 26.

Exemple 4 Montrer que $300^{3000} - 1$ est divisible par 1001.

Réponse

La décomposition de 1001 en produit de facteurs premiers est : $1001 = 7 \times 11 \times 13$, donc si un nombre est divisible par 7, par 11 et par 13, il est divisible par leur produit 1001.

Montrons que $300^{3000} - 1$ est divisible par 7, par 11 et par 13.

Les nombres 7, 11 et 13 sont premiers et ne divisent pas 300.

Par ailleurs $300^{3000} = (300^6)^{500}$ et $300^{3000} = (300^{10})^{300}$ et $300^{3000} = (300^{12})^{250}$.

D'après le petit théorème de Fermat, on déduit :

$300^{3000} = (300^6)^{500} \equiv 1^{500} \equiv 1 \pmod{7}$, donc $300^{3000} - 1$ divisible par 7.

$300^{3000} = (300^{10})^{300} \equiv 1^{300} \equiv 1 \pmod{11}$, donc $300^{3000} - 1$ divisible par 11.

$300^{3000} = (300^{12})^{250} \equiv 1^{250} \equiv 1 \pmod{13}$, donc $300^{3000} - 1$ divisible par 13.

Conclusion

Le nombre $300^{3000} - 1$ étant divisible par les facteurs premiers 7, 11 et 13 est divisible par leur produit 1001.

Cours : Divisibilité dans $\mathbb{Z}$

Résumé

Définition de la relation de congruence modulo n (n dans $\mathbb{N}^*$)

Soit n un entier naturel non nul donné ;

soient x et y deux entiers relatifs quelconques.

On dit que x est congru à y modulo n si la différence $x - y$ est un multiple de n et on note :

$x \equiv y \pmod{n}$ ou encore $x \equiv y \ [n]$ ou encore $x \equiv y \ (n)$

$x \equiv y \pmod{n} \Leftrightarrow x - y$ multiple de n.

Propriété des congruences

▶ compatibilité avec l'addition et la soustraction dans $\mathbb{Z}$: **si** $x \equiv y \ [n]$ et $x' \equiv y' \ [n]$

alors $x + x' \equiv y + y' \ [n]$ et $x - x' \equiv y - y' \ [n]$

▶ compatibilité avec la multiplication et l'élévation à une même puissance dans $\mathbb{Z}$:

si $x \equiv y \ [n]$ et $x' \equiv y' \ [n]$

alors $xx' \equiv yy' \ [n]$ et $x^p \equiv y^p \ [n]$ (p dans $\mathbb{N}$)

▶ simplification d'une congruence : soient x et y deux entiers divisibles par un même entier naturel k ;

- si ($x \equiv y \ [n]$ et n divisible par k) alors $\frac{x}{k} \equiv \frac{y}{k} \ \left[\frac{n}{k}\right]$ (on divise aussi le module)
- si ($x \equiv y \ [n]$ et n et k premiers entre eux) alors $\frac{x}{k} \equiv \frac{y}{k} \ [n]$

▶ un entier relatif a est congru modulo n au reste obtenu dans la division euclidienne de a par n

▶ $x \equiv y \ [n] \Leftrightarrow$ x et y ont le même reste dans la division euclidienne par n

Le petit théorème de Fermat

Si p est un nombre premier et a un entier naturel non divisible par p, alors $a^{p-1} \equiv 1 \pmod{p}$.