

Arithmétique

Maths Expertes

maths-mde.fr
Cours à imprimer pour élève

Lycée Evariste Galois

I. Divisibilité

Définition

Un nombre relatif a est *divisible* par un entier naturel n non nul s'il existe un entier k tel que $a = kn$.

$$a \in \mathbb{Z}, n \in \mathbb{N}^*, a \text{ divisible par } n \iff \exists k \in \mathbb{N}^*, a = kn.$$

n est alors appelé un *diviseur* de a .

Exemple

- 786 est divisible par 2 et par 3 car $786 = 2 \times 393$ et $786 = 3 \times 262$.
- 0 est divisible par tout entier naturel n non nul car $0 = k \times 0$.

Définition

L'ensemble des entiers naturels compris entre deux entiers naturels a et b est noté :

$$[[a ; b]].$$

Exemple

$$[[0 ; 5]] = \{0; 1; 2; 3; 4; 5\}.$$

Propriété

Soit n un entier relatif non nul.

L'ensemble des diviseurs positifs de n est un ensemble fini.

Démonstration

$\llbracket 1 ; |n| \rrbracket$ est un ensemble fini et si n possède des diviseurs alors ils appartiennent à cet ensemble.

Par conséquent, l'ensemble des diviseurs positifs de n est un sous-ensemble de $\llbracket 1 ; |n| \rrbracket$, et est donc fini.

Propriété

Soient a , b et c trois entiers relatifs, $a \neq 0$ et $b \neq 0$.

- ❶ Si a divise b et b divise c alors a divise c .
- ❷ Si a divise b et c alors a divise toute combinaison linéaire de b et c .

Démonstration

« a divise b » peut aussi s'écrire « $a|b$ ».

- ❶ $a|b \iff \exists k \in \mathbb{N}^*, b = ka.$
 $b|c \iff \exists k' \in \mathbb{N}^*, c = k'b.$

Ainsi,

$$\exists(k, k') \in \mathbb{N}^* \times \mathbb{N}^*, c = k' \times ka = (kk')a.$$

Par conséquent, il existe un entier $K = kk'$ tel que $c = Ka$, donc $a|c$.

- ❷ $a|b$ et $a|c$ donc il existe deux entiers k et k' tels que $b = ka$ et $c = k'a$.
 Une combinaison linéaire de b et c est $pb + qc$, p et q étant deux entiers relatifs.

II. Division euclidienne

Théorème

Soient a et b deux entiers naturels.

Il existe un unique couple $(q; r)$ d'entiers naturels tels que :

$$a = bq + r, \quad 0 \leq r < b.$$

Cette dernière écriture est appelée la *division euclidienne de a par b* .
 q est alors le *quotient* et r le *reste* de cette division.

Démonstration

Existence : La partie entière d'un réel x est l'entier relatif n tel que
 $n \leq x < n + 1$. On note $n = E(x)$.

Posons alors $q = E\left(\frac{a}{b}\right)$. Or, $\frac{a}{b} \geq 0$, ainsi $E\left(\frac{a}{b}\right) \geq 0$.

Nous avons alors par définition,

$$q \leq \frac{a}{b} < q + 1 \Leftrightarrow qb \leq a < bq + b \Leftrightarrow 0 \leq a - bq < b, \text{ et cela car } b > 0.$$

En posant, $r = a - bq$, on obtient d'une part, $a = bq + r$ et d'autre part
 $0 \leq r < b$.

L'existence d'un couple $(q; r)$ vérifiant les conditions précitées est ainsi prouvée.

Unicité : Supposons qu'il existe deux couples d'entiers naturels $(q; r)$ et

$$(q'; r') \text{ tels que : } \begin{cases} a = bq + r, & \text{avec } 0 \leq r < b. \\ a = bq' + r', & \text{avec } 0 \leq r' < b. \end{cases}$$

Ce qui revient à dire, $bq + r = bq' + r'$. Soit, $b(q - q') = r' - r$.

Autrement dit, $b|(r - r')$. Or,

$$\begin{cases} 0 \leq r < b \\ 0 \leq r' < b \end{cases} \Leftrightarrow \begin{cases} 0 \leq r < b \\ -b < -r' \leq 0. \end{cases}$$

Ce qui implique que $-b < r - r' < b$. Et, ce dernier résultat n'est possible que si $r - r' = 0$ soit $r = r'$.

Par ailleurs, $b(q - q') = r' - r = 0$ et cela entraîne que $q = q'$. D'où l'unicité.

Exemple

La division euclidienne de 37 par 11 est : $37 = 3 \times 11 + 4$. Le quotient de cette division est 3, et le reste 4.

Propriété

Soit b un entier naturel tel que $b \geq 2$. Tout entier a s'écrit sous une, et une seule, des formes bq , $bq + 1$, $bq + 2$, $\dots$, $bq + (b - 1)$, où q est un entier.

Démonstration

Soit a un entier.

En effectuant la division euclidienne de a par b non nul, il existe deux entiers naturels q et r tels que $a = bq + r$ avec $0 \leq r < b$.

Par unicité du quotient et du reste $a = bq$, ou $a = bq + 1$, $\dots$, ou $a = bq + (b - 1)$.

Exemple

Soit n un entier naturel. Posons $A = n(n-2)(n+2)$. Démontrer que A est un multiple de 3.

Preuve : Soit n un entier naturel. Il y a trois cas possible.

1^{er} cas : il existe $k \in \mathbb{N}$ tel que $n = 3k$. Ainsi,
 $A = 3k(3k-2)(3k+2) = 3[k(3k-2)(3k+2)]$, ce qui entraine que A est divisible par 3.

2^{ème} cas : il existe $k \in \mathbb{N}$ tel que $n = 3k + 1$. Ainsi,
 $A = (3k+1)(3k-1)(3k+3) = 3[(3k+1)(3k-1)(k+1)]$ et cela entraine que A est divisible par 3.

3^{ème} cas : il existe $k \in \mathbb{N}$ tel que $n = 3k + 2$. Ainsi,
 $A = (3k+2)(3k)(3k+4) = 3[(3k+2)k(3k+4)]$ et cela entraine que A est divisible par 3.

III. Congruences

Introduction : Activité - Corrigé

Définition

Soient m un entier naturel non nul, et a et b deux entiers relatifs.

On dit que a et b sont congrus modulo m lorsqu'ils ont le même reste dans division euclidienne par m .

On dit aussi que a est congru à b modulo m .

On note alors :

$$a \equiv b \quad [m] \quad \text{ou} \quad a \equiv b \quad (m) \quad \text{ou} \quad a \equiv b \quad \text{mod } m.$$

Exemples

- $21 = 2 \times 10 + 1$ et $15 = 2 \times 7 + 1$, donc

$$21 \equiv 15 \quad [2] \quad \text{ou} \quad 21 \equiv 15 \quad (2) \quad \text{ou} \quad 21 \equiv 15 \quad \text{mod } 2.$$

- $21 = 4 \times 5 + 1$ et $17 = 4 \times 4 + 1$, donc

$$21 \equiv 17 \quad [4] \quad \text{ou} \quad 21 \equiv 17 \quad (4) \quad \text{ou} \quad 21 \equiv 17 \quad \text{mod } 4.$$

- $21 = 3 \times 6 + 3$ et $33 = 5 \times 6 + 3$, donc

$$21 \equiv 33 \quad [3] \quad \text{ou} \quad 21 \equiv 33 \quad (3) \quad \text{ou} \quad 21 \equiv 33 \quad \text{mod } 3.$$

Propriétés

Soient a et b deux entiers relatifs, et n un entier naturel.

- ➊ **Divisibilité** : $a \equiv b \pmod{n} \iff n \mid (a - b)$.
- ➋ **Transitivité** : Si $a \equiv c \pmod{n}$ et $c \equiv b \pmod{n}$ alors $a \equiv b \pmod{n}$, pour $c \in \mathbb{Z}$.
- ➌ **Somme** :
 - a. $a \equiv b \pmod{n} \iff a + k \equiv b + k \pmod{n}$ pour $k \in \mathbb{Z}$.
 - b. $\begin{cases} a \equiv b \pmod{n} \\ a' \equiv b' \pmod{n} \end{cases} \implies a + a' \equiv b + b' \pmod{n}$.
- ➍ **Produit** :
 - a. $a \equiv b \pmod{n} \iff ka \equiv kb \pmod{n}$ pour $k \in \mathbb{Z}$.
 - b. $\begin{cases} a \equiv b \pmod{n} \\ a' \equiv b' \pmod{n} \end{cases} \implies aa' \equiv bb' \pmod{n}$.
- ➎ **Puissance** : $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$ pour $k \in \mathbb{N}^*$.

Démonstration

$\forall a, b \in \mathbb{Z}$ et $\forall n \in \mathbb{N}$.

- ① **Divisibilité :** $[\Rightarrow] a \equiv b [n]$ revient à dire que a et b ont le même reste r dans la division euclidienne par n . Ainsi, il existe deux entiers

$$k \text{ et } k' \text{ tels que : } \begin{cases} a = nk + r \\ b = nk' + r \end{cases}.$$

En soustrayant membre à membre les deux égalités, on obtient :
 $a - b = n(k - k')$. Ainsi, $n|a - b$.

Divisibilité : $[\Leftarrow]$ Supposons que $n|a - b$.

Il existe deux couples d'entiers naturels $(q; r)$ et $(q'; r')$ tels que :

$$\begin{cases} a = nq + r, & \text{avec } 0 \leq r < n \\ b = nq' + r', & \text{avec } 0 \leq r' < n \end{cases}.$$

En soustrayant membre à membre les deux égalités, on obtient :

$$a - b = n(q - q') + (r - r'), \text{ où } -n < r - r' < n.$$

Or, $n|a - b$. Ainsi, $n|r - r'$. Et cela n'est possible que si $r = r'$.

a et b ont le même reste dans la division euclidienne par n . Donc
 $a \equiv b [n]$.

- ② **Transitivité :**

Si $a \equiv c [n]$ et $c \equiv b [n]$ alors $n|a - c$ et $n|c - b$.

Et donc, $n|a - c + c - b$, soit $n|a - b$.

Autrement dit, $a \equiv b [n]$.

- ③ **Somme :**

a. Soit $k \in \mathbb{Z}$.

$$a \equiv b [n] \Leftrightarrow n|a - b \Leftrightarrow n|a + k - (k + b) \Leftrightarrow n + k \equiv b + k [n].$$

$$\text{b. } \begin{cases} a \equiv b [n] \\ a' \equiv b' [n] \end{cases} \implies \begin{cases} n|a - b \\ n|a' - b' \end{cases} \implies n|a + a' - (b + b') \implies a + a' \equiv b + b' [n].$$

④ **Produit :**

$$\begin{aligned}
 \text{a. } a \equiv b [n] &\iff n \mid (a - b) \\
 &\iff n \mid k(a - b), \forall k \in \mathbb{Z} \\
 &\iff n \mid ka - kb, \forall k \in \mathbb{Z} \\
 &\iff ka \equiv kb [n], \forall k \in \mathbb{Z}. \\
 \text{b. } \begin{cases} a \equiv b [n] \\ a' \equiv b' [n] \end{cases} &\implies \begin{cases} \exists k \in \mathbb{N} \mid a = b + kn \\ \exists k' \in \mathbb{N} \mid a' = b' + k'n \end{cases} \\
 &\implies aa' = (b + kn)(b' + k'n) \\
 &\implies aa' = bb' + n[bk' + k'b + kk'n'] \\
 &\implies aa' \equiv bb' [n].
 \end{aligned}$$

⑤ **Puissance :**

Démontrons par récurrence que $a \equiv b [n] \implies a^k \equiv b^k [n]$ pour $k \in \mathbb{Z}$.

- **Initialisation :** pour $k = 1$, $a \equiv b [n] \implies a^1 \equiv b^1 [n]$.
- **Hérédité :** supposons que pour un entier k fixé,
 $a \equiv b [n] \implies a^k \equiv b^k [n]$,
 $\implies aa^k \equiv bb^k [n]$
 $\implies a^{k+1} \equiv b^{k+1} [n]$.

L'hérédité est alors vérifiée.

Exemple

On a : $17 \equiv 1 \pmod{4}$. Alors,

$$\forall k \in \mathbb{N}, \quad 17^k \equiv 1^k \pmod{4}$$

soit,

$$\forall k \in \mathbb{N}, \quad 17^k \equiv 1 \pmod{4}.$$

IV. PGCD de deux entiers

Définition

Soient a et b deux entiers naturels non tous les deux nuls.

Le *plus grand commun diviseur* de a et b , noté $a \wedge b$ ou $PGCD(a; b)$, est le plus grand diviseur de a et de b .

Exemple

Les diviseurs de 12 sont : 1, 2, 3, 4, 6, 12.

Les diviseurs de 15 sont : 1, 3, 5.

Ainsi, $12 \wedge 15 = 3$ car 3 divise 12 et 15, et c'est le plus grand des diviseurs communs qui apparaît dans les deux listes.

Propriété

Soient a et b deux entiers naturels non nuls tels que :

$\exists q \in \mathbb{N}^*, a = bq + r, \quad 0 \leq r < b$. Alors, $a \wedge b = b \wedge r$.

Démonstration

Soit d un diviseur commun à a et b . On a par définition $a = qb + r$, alors $r = a - qb$.

r s'écrit comme une combinaison linéaire de a et de b , donc d divise r .

De même a est une combinaison linéaire de b et de r , donc tout diviseur commun à b et r divise a .

Ainsi, l'ensemble des diviseurs communs à a et b est confondu avec l'ensemble des diviseurs communs à b et r . Ces deux ensembles ont donc le même plus grand élément. Par conséquent, $a \wedge b = b \wedge r$.

Algorithme d'Euclide

On définit par récurrence la suite des entiers $r_0, r_1, \dots, r_n$ tels que :

r_0 est le reste de la division euclidienne de a par b .

Si $r_0 \neq 0$, r_1 est le reste de la division euclidienne de b par r_0 .

Pour tout $k \in \{1; \dots; n-1\}$, si $r_k \neq 0$, alors r_{k+1} est le reste de la division euclidienne de r_{k-1} par r_k .

Alors, cette suite d'entiers est nulle à partir d'un certain rang et la dernière valeur non nul prise par cette suite est $a \wedge b$.

Démonstration

Soit r_0 le reste de la division euclidienne de a par b . Par définition du reste d'une division euclidienne, $0 \leq r_0 < b$ et on sait que $a \wedge b = b \wedge r_0$.

Soit $m \in \mathbb{N}$. Supposons qu'on ait construit $r_0, r_1, \dots, r_{m-1}$ non nuls et r_m tels que pour tout $k \in \{1; \dots; m-1\}$, r_{k+1} soit le reste de la division euclidienne de r_{k-1} par r_k .

Alors, $0 \leq r_m < r_{m-1} < \dots < b$ et $a \wedge b = b \wedge r_0 = \dots = r_{m-1} \wedge r_m$.

Si $r_m = 0$ alors $r_{m-1} \wedge r_m = r_{m-1}$.

La suite d'entiers naturels (r_m) est strictement décroissante et minorée par 0. Elle est donc nulle à partir d'un certain rang.

Soit alors n_0 tel que $r_{n_0} = 0$ et $r_{n_0-1} > 0$.

Ainsi, par construction, $a \wedge b = b \wedge r_0 = \dots = r_{n_0-1} \wedge r_{n_0} = r_{n_0-1}$.

Exemple

Prenons $a = 1\,386$ et $b = 1\,092$.

- $1\,386 = 1 \times 1\,092 + 294$.
Ainsi, $1\,386 \wedge 1\,092 = 1\,092 \wedge 294$.
- $1\,092 = 3 \times 294 + 210$.
Ainsi, $1\,092 \wedge 294 = 294 \wedge 210$.
- $294 = 1 \times 210 + 84$.
Ainsi, $294 \wedge 210 = 210 \wedge 84$.
- $210 = 2 \times 84 + 42$.
Ainsi, $210 \wedge 84 = 84 \wedge 42$.
- $84 = 2 \times 42 + 0$.
Ainsi, $84 \wedge 42 = 42 \wedge 0 = 42$.

On en déduit alors que : $1\,386 \wedge 1\,092 = 42$.

Propriété

Pour tous entiers naturels non nuls a , b et k , on a $ka \wedge kb = k \times a \wedge b$.

Démonstration

La division euclidienne de a par b est donnée par l'écriture unique :
 $a = bq + r$ avec $0 \leq r < b$.

Notons r_n le dernier reste non nul des divisions euclidiennes effectuées selon l'algorithme d'Euclide.

Par ailleurs, on peut écrire, $ka = kbp + kr$ avec $0 \leq r < b$. En appliquant l'algorithme d'Euclide, le dernier reste non nul est alors kr_n .

Ainsi, on a bien $PGCD(ka; kb) = kPGCD(a; b)$.

Propriétés

Soient a et b deux entiers naturels.

- ❶ Si d divise a et d divise b alors d divise $a \wedge b$.
- ❷ Deux entiers sont premiers entre eux si et seulement si $a \wedge b = 1$.
- ❸ Il existe deux entiers naturels a' et b' tels que $a = a' \times a \wedge b$ et $b = b' \times a \wedge b$, avec $a' \wedge b' = 1$.

Démonstration

- ❶ Soit d un diviseur commun. Par l'algorithme d'Euclide, d divise les restes successifs des divisions euclidiennes et donc également le dernier reste non nul qui est le PGCD de a et de b .
- ❷
 - Si a et b sont premiers entre eux, leur seul diviseur commun est 1, donc $a \wedge b = 1$.
 - Si $a \wedge b = 1$ alors le plus grand diviseur commun de a et b est 1, donc le seul diviseur commun est 1. Et donc a et b sont premiers entre eux.
- ❸ Soient $d' = a' \wedge b'$ et k_1 et k_2 les entiers tels que $a' = d'k_1$ et $b' = d'k_2$.
On doit montrer que $d' = 1$
On a, $a = d'k_1 a \wedge b$ et $b = d'k_2 a \wedge b$ donc $d' a \wedge b$ est un diviseur commun de a et b .
Ainsi, $d' a \wedge b \leq a \wedge b$. Par conséquent, $d' = 1$ (car $d > 0$).

V. Théorème de Bézout et théorème de Gauss

Théorème de Bézout

Soient a et b deux entiers naturels non nuls.

$$a \wedge b = 1 \iff \exists (u; v) \in \mathbb{Z}^2, au + bv = 1.$$

Démonstration

- Démontrons d'abord que si il existe un couple $(u; v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ alors $a \wedge b = 1$.

Supposons donc qu'il existe un couple $(u; v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.
 $a \wedge b$ divise a et b , donc divise $au + bv$, donc 1. Or, 1 n'a qu'un diviseur : lui-même.
 Donc $a \wedge b = 1$.

- Supposons maintenant que $a \wedge b = 1$.
 Notons E l'ensemble des combinaisons linéaires de a et b , strictement positives. E n'est pas vide car
 $a = 1 \times a + 0 \times b$ appartient à E .
 E a donc un plus petit élément, que l'on va noter $c = au + bv$.
 La division euclidienne de a par c est : $a = cq + r$, $0 \leq r < c$.
 Ainsi,

$$r = a - cq = a - (au + bv)q = (1 - uq)a + (-vq)b.$$

r est donc une combinaison linéaire de a et b , donc appartient à E . Mais $r < c$, ce qui est contradictoire avec notre hypothèse. Cela implique alors que $r = 0$, et donc c divise a .

De manière analogue, on montre que c divise b et donc que c est un diviseur commun à a et b . Or, $a \wedge b = 1$ donc $c = 1$, soit $au + bv = 1$.

Identité de Bézout

Soient a et b deux entiers naturels non nuls.

$$a \wedge b = d \implies \exists (u; v) \in \mathbb{Z}^2, \quad au + bv = d.$$

Démonstration

Soient a et b deux entiers relatifs non nuls et on pose $d = a \wedge b$.

Il existe deux entiers a' et b' tels que $a = a'd$ et $b = b'd$ et tels que $a' \wedge b' = 1$.

D'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $a'u + b'v = 1$.

On obtient alors, $au + bv = a'du + b'dv = d(a'u + b'v) = d$.

Théorème de Gauss

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

Si a divise bc et si $a \wedge b = 1$ alors a divise c .

Démonstration

a divise bc donc il existe un entier k non nul tel que $bc = ak$.

$a \wedge b = 1$ donc d'après le théorème de Bézout, il existe un couple $(u; v)$ d'entiers relatifs tel que $au + bv = 1$, soit en multipliant par c :

$$acu + bcv = c \iff acu + akv = c \iff a(cu + kv) = c.$$

Ainsi, a divise c .

Propriété

Soient a et b deux entiers naturels.

$$a \wedge b \times a \vee b = ab.$$

Démonstration

Par définition $a \vee b$ est un multiple de a , il existe alors un entier naturel (minimal) k tel que $a \vee b = ka$.

Par ailleurs, il existe a' et b' dans $\mathbb{N}$ tels que $a = a' \times a \wedge b$ et $b = b' \times a \wedge b$ avec $a' \wedge b' = 1$.

Dès lors, $b \mid ka \implies b' a \wedge b \mid ka' a \wedge b \implies b' \mid ka'$.

Or, $b' \wedge a' = 1$. Ainsi, selon le théorème de Gauss $b' \mid k$. Autrement dit, il existe un entier naturel q tel que $k = qb'$. k est minimal si $q = 1$.

Par conséquent, $a \wedge b \times a \vee b = a \wedge b \times b' a = ab$.

VI. Nombres premiers

Définition

Un entier naturel est premier s'il n'est divisible que par 1 et lui-même.

Remarque

Notez bien dans la définition la présence de la conjonction « et » qui induit nécessairement que le nombre doit admettre exactement deux diviseurs.

Ainsi, le nombre 1 n'est pas premier car il n'admet qu'un diviseur : lui-même.

Théorème

Il existe une infinité de nombres premiers.

Démonstration

Supposons que l'ensemble des nombres premiers soit fini. Notons alors cet ensemble :

$$\{p_1; p_2; \dots; p_n\}.$$

Considérons alors le nombre :

$$N = p_1 \times p_2 \times \dots \times p_n + 1.$$

Il est immédiat que N n'appartient pas à l'ensemble des nombres premiers considéré.

Or, N n'est divisible par aucun des p_k , pour $1 \leq k \leq n$.

Par conséquent, il est premier. Ce qui est contradictoire avec le fait que N n'appartient pas à l'ensemble des nombres premiers considéré.

Ainsi, notre hypothèse selon laquelle l'ensemble des nombres premiers est fini est fausse.

Propriété

Soit n un entier naturel non nul.

Si n n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$ alors n est premier.

Démonstration

Si n n'est pas premier, l'ensemble D des diviseurs stricts de n n'est pas vide. D'après le principe du bon ordre, D admet donc un plus petit élément p .

Si p n'était pas premier, il admettrait un diviseur strict d qui diviserait n . Ceci est impossible car p est le plus petit élément de D . Donc p est premier. n admet donc un diviseur premier p tel que $p \geq 2$ et $n = pq$ avec $p \leq q$.

Ainsi, $p^2 \leq pq \Leftrightarrow p^2 \leq n$. D'où le résultat.

Exemple

$\sqrt{137} \approx 11,7$. De plus, 137 n'est pas divisible par 2, 3, 5, 7 et 11 donc $137 \in \mathbb{P}$ avec $\mathbb{P}$ l'ensemble des nombres premiers.

Théorème

Tout entier naturel n supérieur ou égal à 2 peut s'écrire sous la forme :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$$

où k est un entier naturel non nul et $p_i \in \mathbb{P}$ pour $1 \leq i \leq k$.

Cette écriture est appelée la décomposition en produit de facteurs premiers de n et elle est unique.

VII. Petit théorème de Fermat

Petit théorème de Fermat

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

Démonstration

On considère les $(p-1)$ premiers multiples de a : $a, 2a, 3a, \dots, (p-1)a$,
 et on note : $r_1, r_2, r_3, \dots, r_{p-1}$, les restes des divisions euclidiennes des
 susdits multiples par p .

Ces restes sont deux à deux distincts. En effet, si on suppose l'existence de
 deux restes identiques, r_i et r_j avec $i > j$, alors :

$ia - ja \equiv r_i - r_j \pmod{p} \Leftrightarrow a(i-j) \equiv 0 \pmod{p}$. Autrement dit, $p \mid a(i-j)$.

D'après le théorème de Gauss, cela implique que $p \mid a$ ou $p \mid (i-j)$. C'est
 contradictoire avec le fait a n'est pas un multiple de p et $i-j < p$.

On déduit alors que : $r_1 \times r_2 \times \dots \times r_{p-1} = (p-1)!$.

Dès lors,

$$\begin{aligned} a \times 2a \times \dots \times (p-1)a &\equiv (p-1)! \pmod{p} \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod{p} \\ (a^{p-1} - 1)(p-1)! &\equiv 0 \pmod{p}. \end{aligned}$$

Or, $(p-1)!$ est premier avec p car tous les facteurs de $(p-1)!$ sont
 inférieurs à p , alors d'après le théorème de Gauss, on a :

$$a^{p-1} - 1 \equiv 0 \pmod{p} \Leftrightarrow a^{p-1} \equiv 1 \pmod{p}.$$

Exemple

Prenons $a = 27$ et $p = 5$.

p est premier et a n'est pas divisible par p donc $27^4 \equiv 1 \pmod{5}$.

Remarque

La congruence de ce théorème est aussi présentée sous la forme suivante :

$$a^p \equiv a \pmod{p}.$$