L'impossible, il n'y a que ça de vrai : l'envers du décor mathématique

Rémi Carles

CNRS & Univ. Rennes

Des évidences... ?

Je crois que deux et deux sont quatre, Sganarelle, et que quatre et quatre sont huit.

Molière, Don Juan, III, 1

5ᵉ postulat d'Euclide, version Proclus :

Par un point donné hors d'une droite, on peut mener une et une seule parallèle à cette droite.

Des évidences... ?

> *Je crois que deux et deux sont quatre, Sganarelle, et que quatre et quatre sont huit.*
>
> Molière, Don Juan, III, 1

5$^{\text{e}}$ postulat d'Euclide, version Proclus :

> *Par un point donné hors d'une droite, on peut mener une et une seule parallèle à cette droite.*

Des évidences... ?

> *Je crois que deux et deux sont quatre, Sganarelle, et que quatre et quatre sont huit.*
>
> Molière, Don Juan, III, 1

5^{e} postulat d'Euclide, version Proclus :

> *Par un point donné hors d'une droite, on peut mener une et une seule parallèle à cette droite.*

Des évidences remises en cause

- Copernic, Galilée,

  Pour voir que c'est bien le soleil qui tourne autour de la terre, il suffit tout de même d'ouvrir les yeux. Il n'y a pas besoin de calculs, il suffit de notre gros bon sens espagnol.

  Paul Claudel, Le soulier de satin, Troisième journée, Scène II

- Darwin,
- Camus,
- Einstein,
- Picasso,
- Schönberg,
- etc.

Des évidences remises en cause

- Copernic, Galilée,

  Pour voir que c'est bien le soleil qui tourne autour de la terre, il suffit tout de même d'ouvrir les yeux. Il n'y a pas besoin de calculs, il suffit de notre gros bon sens espagnol.

  Paul Claudel, Le soulier de satin, Troisième journée, Scène II

- Darwin,
- Camus,
- Einstein,
- Picasso,
- Schönberg,
- etc.

Des évidences remises en cause

- Copernic, Galilée,

  Pour voir que c'est bien le soleil qui tourne autour de la terre, il suffit tout de même d'ouvrir les yeux. Il n'y a pas besoin de calculs, il suffit de notre gros bon sens espagnol.

  Paul Claudel, Le soulier de satin, Troisième journée, Scène II

- Darwin,
- Camus,
- Einstein,
- Picasso,
- Schönberg,
- etc.

Des évidences remises en cause

- Copernic, Galilée,

  Pour voir que c'est bien le soleil qui tourne autour de la terre, il suffit tout de même d'ouvrir les yeux. Il n'y a pas besoin de calculs, il suffit de notre gros bon sens espagnol.

  Paul Claudel, Le soulier de satin, Troisième journée, Scène II

- Darwin,
- Camus,
- Einstein,
- Picasso,
- Schönberg,
- etc.

Des évidences remises en cause

- Copernic, Galilée,

  Pour voir que c'est bien le soleil qui tourne autour de la terre, il suffit tout de même d'ouvrir les yeux. Il n'y a pas besoin de calculs, il suffit de notre gros bon sens espagnol.

  Paul Claudel, Le soulier de satin, Troisième journée, Scène II

- Darwin,
- Camus,
- Einstein,
- Picasso,
- Schönberg,
- etc.

Des évidences remises en cause

- Copernic, Galilée,

  Pour voir que c'est bien le soleil qui tourne autour de la terre, il suffit tout de même d'ouvrir les yeux. Il n'y a pas besoin de calculs, il suffit de notre gros bon sens espagnol.

  Paul Claudel, Le soulier de satin, Troisième journée, Scène II

- Darwin,
- Camus,
- Einstein,
- Picasso,
- Schönberg,
- etc.

Des évidences remises en cause

- Copernic, Galilée,

  Pour voir que c'est bien le soleil qui tourne autour de la terre, il suffit tout de même d'ouvrir les yeux. Il n'y a pas besoin de calculs, il suffit de notre gros bon sens espagnol.

  Paul Claudel, Le soulier de satin, Troisième journée, Scène II

- Darwin,
- Camus,
- Einstein,
- Picasso,
- Schönberg,
- etc.

Des évidences remises en cause

- Copernic, Galilée,

  Pour voir que c'est bien le soleil qui tourne autour de la terre, il suffit tout de même d'ouvrir les yeux. Il n'y a pas besoin de calculs, il suffit de notre gros bon sens espagnol.

  Paul Claudel, Le soulier de satin, Troisième journée, Scène II

- Darwin,
- Camus,
- Einstein,
- Picasso,
- Schönberg,
- etc.

$1+1=?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9 \equiv 0[9]$.

Exemple

$3 \equiv 3[9]$.
$10 \equiv 1[9] \rightsquigarrow 10+3 \equiv 4[9]$.

Reste de la division euclidienne : $a \equiv b[9]$ signifie $a = 9n + b$, pour un nombre entier n. $0 \leqslant b < 9$ est le reste de la division euclidienne. . .ou encore portion congrue.

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne...ou encore portion congrue.

La preuve par 9 : condition nécessaire.

Exemple ($17\times 35=595$)

$\rightsquigarrow 1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow 5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1 + 1 = ?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1 + 7 = 8$, $3 + 5 = 8$, $8 \times 8 = 64$, et $6 + 4 = 10$. Enfin, $1 + 0 = 1$.
$\rightsquigarrow$ $5 + 9 + 5 = 19$, $1 + 9 = 10$ et $1 + 0 = 1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9 = 0$.
Notion de congruence : $9 \equiv 0[9]$.

Exemple

$3 \equiv 3[9]$.
$10 \equiv 1[9] \rightsquigarrow 10 + 3 \equiv 4[9]$.

Reste de la division euclidienne : $a \equiv b[9]$ signifie $a = 9n + b$, pour un nombre entier n. $0 \leqslant b < 9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1 + 1 = ?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1 + 7 = 8$, $3 + 5 = 8$, $8 \times 8 = 64$, et $6 + 4 = 10$. Enfin, $1 + 0 = 1$.
$\rightsquigarrow$ $5 + 9 + 5 = 19$, $1 + 9 = 10$ et $1 + 0 = 1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9 = 0$.
Notion de congruence : $9 \equiv 0[9]$.

Exemple

$3 \equiv 3[9]$.
$10 \equiv 1[9] \rightsquigarrow 10 + 3 \equiv 4[9]$.

Reste de la division euclidienne : $a \equiv b[9]$ signifie $a = 9n + b$, pour un nombre entier n. $0 \leqslant b < 9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1 + 1 = ?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1 + 7 = 8$, $3 + 5 = 8$, $8 \times 8 = 64$, et $6 + 4 = 10$. Enfin, $1 + 0 = 1$.

$\rightsquigarrow$ $5 + 9 + 5 = 19$, $1 + 9 = 10$ et $1 + 0 = 1$.

La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9 = 0$.

Notion de congruence : $9 \equiv 0[9]$.

Exemple

$3 \equiv 3[9]$.

$10 \equiv 1[9] \rightsquigarrow 10 + 3 \equiv 4[9]$.

Reste de la division euclidienne : $a \equiv b[9]$ signifie $a = 9n + b$, pour un nombre entier n. $0 \leqslant b < 9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1+1=?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne. . .ou encore portion congrue.

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1+1=?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne. . .ou encore portion congrue.

La preuve par 9 : condition nécessaire.

Exemple ($17\times 35=595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne...ou encore portion congrue.

$1+1=?$

La preuve par 9 : condition nécessaire.

Exemple ($17\times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1 + 1 = ?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1 + 7 = 8$, $3 + 5 = 8$, $8 \times 8 = 64$, et $6 + 4 = 10$. Enfin, $1 + 0 = 1$.
$\rightsquigarrow$ $5 + 9 + 5 = 19$, $1 + 9 = 10$ et $1 + 0 = 1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9 = 0$.
Notion de congruence : $9 \equiv 0[9]$.

Exemple

$3 \equiv 3[9]$.
$10 \equiv 1[9]$ $\rightsquigarrow$ $10 + 3 \equiv 4[9]$.

Reste de la division euclidienne : $a \equiv b[9]$ signifie $a = 9n + b$, pour un nombre entier n. $0 \leqslant b < 9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1 + 1 = ?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1 + 7 = 8$, $3 + 5 = 8$, $8 \times 8 = 64$, et $6 + 4 = 10$. Enfin, $1 + 0 = 1$.
$\rightsquigarrow$ $5 + 9 + 5 = 19$, $1 + 9 = 10$ et $1 + 0 = 1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9 = 0$.
Notion de congruence : $9 \equiv 0[9]$.

Exemple

$3 \equiv 3[9]$.
$10 \equiv 1[9] \rightsquigarrow 10 + 3 \equiv 4[9]$.

Reste de la division euclidienne : $a \equiv b[9]$ signifie $a = 9n + b$, pour un nombre entier n. $0 \leqslant b < 9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1+1=?$

La preuve par 9 : condition nécessaire.

Exemple ($17\times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne. . .ou encore portion congrue.

$1+1=?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8 \times 8 = 64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9 \equiv 0[9]$.

Exemple

$3 \equiv 3[9]$.
$10 \equiv 1[9] \rightsquigarrow 10+3 \equiv 4[9]$.

Reste de la division euclidienne : $a \equiv b[9]$ signifie $a = 9n + b$, pour un nombre entier n. $0 \leqslant b < 9$ est le reste de la division euclidienne. . . ou encore portion congrue.

$1+1=?$

La preuve par 9 : condition nécessaire.

Exemple ($17 \times 35 = 595$)

$\rightsquigarrow$ $1+7=8$, $3+5=8$, $8\times 8=64$, et $6+4=10$. Enfin, $1+0=1$.
$\rightsquigarrow$ $5+9+5=19$, $1+9=10$ et $1+0=1$.
La preuve par 9 est *encourageante* : on trouve 1 dans les deux cas.

Le principe de la preuve par 9 : $9=0$.
Notion de congruence : $9\equiv 0[9]$.

Exemple

$3\equiv 3[9]$.
$10\equiv 1[9] \rightsquigarrow 10+3\equiv 4[9]$.

Reste de la division euclidienne : $a\equiv b[9]$ signifie $a=9n+b$, pour un nombre entier n. $0\leqslant b<9$ est le reste de la division euclidienne. . .ou encore portion congrue.

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9].$

$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9].$

$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9].$

$595 \equiv$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.

$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.

$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.

$595 \equiv$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.

$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.

$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.

$595 \equiv$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9].$

$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9].$

$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9].$

$595 \equiv$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + 9 + 5[9]$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + \cancel{9} + 5[9]$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + \cancel{9} + 5[9] \equiv 10[9]$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9].$
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9].$
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9].$
$595 \equiv 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9].$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9]$.

Remarque

Si dans une multiplication (ou addition), on se trompe d'un multiple de 9, la preuve par 9 ne le voit pas.

Exemple ($17 \times 35 = 9595!?!$)

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9]$.

Remarque

Si dans une multiplication (ou addition), on se trompe d'un multiple de 9, la preuve par 9 ne le voit pas.

Exemple ($17 \times 35 = 9595!?!$)

On a déjà vu : $17 \times 35 \equiv 1[9]$.

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9]$.

Remarque

Si dans une multiplication (ou addition), on se trompe d'un multiple de 9, la preuve par 9 ne le voit pas.

Exemple ($17 \times 35 = 9595$!?!)

On a déjà vu : $17 \times 35 \equiv 1[9]$.
$9595 \equiv 9 + 5 + 9 + 5[9]$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9]$.

Remarque

Si dans une multiplication (ou addition), on se trompe d'un multiple de 9, la preuve par 9 ne le voit pas.

Exemple ($17 \times 35 = 9595$!?!)

On a déjà vu : $17 \times 35 \equiv 1[9]$.
$9595 \equiv \cancel{9} + 5 + \cancel{9} + 5[9]$

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9]$.

Remarque

Si dans une multiplication (ou addition), on se trompe d'un multiple de 9, la preuve par 9 ne le voit pas.

Exemple ($17 \times 35 = 9595$!?!)

On a déjà vu : $17 \times 35 \equiv 1[9]$.
$9595 \equiv \cancel{9} + 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9]$.

Congruence

En congruence, on peut additionner et multiplier.

Exemple (La preuve par neuf revisitée)

$17 = 10 + 7 \equiv 1 + 7[9] \equiv 8[9]$.
$35 = 3 \times 10 + 5 \equiv 3 + 5[9] \equiv 8[9]$.
$17 \times 35 \equiv 8 \times 8[9] \equiv 64[9] \equiv 6 \times 10 + 4[9] \equiv 6 + 4[9] \equiv 10[9] \equiv 1[9]$.
$595 \equiv 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9]$.

Remarque

Si dans une multiplication (ou addition), on se trompe d'un multiple de 9, la preuve par 9 ne le voit pas.

Exemple ($17 \times 35 = 9595$!?!)

On a déjà vu : $17 \times 35 \equiv 1[9]$.
$9595 \equiv \cancel{9} + 5 + \cancel{9} + 5[9] \equiv 10[9] \equiv 1[9]$.
$\rightsquigarrow$ la preuve par 9 ne voit pas cette (grossière) erreur.

Des généralisations

- Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 =$

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv$

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.

Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv$

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv$

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.

Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv$

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv 1 + 2 + 3 + 4 + 5 + 6[3]$

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$$123456 \equiv 1 + 2 + \cancel{3} + 4 + 5 + \cancel{6}[3]$$

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$$123456 \equiv 1 + 2 + \cancel{3} + 4 + 5 + \cancel{6}[3] \equiv 1 + 2 + 4 + 5[3] \equiv 0[3].$$

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv 1 + 2 + \cancel{3} + 4 + 5 + \cancel{6}[3] \equiv 1 + 2 + 4 + 5[3] \equiv 0[3]$.
$\rightsquigarrow$ 123456 est divisible par 3.

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv 1 + 2 + \cancel{3} + 4 + 5 + \cancel{6}[3] \equiv 1 + 2 + 4 + 5[3] \equiv 0[3]$.
$\rightsquigarrow$ 123456 est divisible par 3.

Exemple

$23456 \equiv 2[3]$: 23456 n'est pas divisible par 3.

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv 1 + 2 + \cancel{3} + 4 + 5 + \cancel{6}[3] \equiv 1 + 2 + 4 + 5[3] \equiv 0[3]$.
$\rightsquigarrow$ 123456 est divisible par 3.

Exemple

$23456 \equiv 2[3]$: 23456 n'est pas divisible par 3.

Remarque (Preuve par 3)

On peut faire comme pour la preuve par 9. . .mais avec davantage de risque de laisser passer une erreur (pourquoi ?).

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.
Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv 1 + 2 + \cancel{3} + 4 + 5 + \cancel{6}[3] \equiv 1 + 2 + 4 + 5[3] \equiv 0[3]$.
$\rightsquigarrow$ 123456 est divisible par 3.

Exemple

$23456 \equiv 2[3]$: 23456 n'est pas divisible par 3.

Remarque (Preuve par 3)

On peut faire comme pour la preuve par 9. . .mais avec davantage de risque de laisser passer une erreur (pourquoi ?).

• Un nombre est-il divisible par 5 ? $5 = 0$.

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.

Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv 1 + 2 + \cancel{3} + 4 + 5 + \cancel{6}[3] \equiv 1 + 2 + 4 + 5[3] \equiv 0[3]$.

$\rightsquigarrow$ 123456 est divisible par 3.

Exemple

$23456 \equiv 2[3]$: 23456 n'est pas divisible par 3.

Remarque (Preuve par 3)

On peut faire comme pour la preuve par 9. . .mais avec davantage de risque de laisser passer une erreur (pourquoi ?).

• Un nombre est-il divisible par 5 ? $5 = 0$.

$10 \equiv 0[5]$

Des généralisations

• Un nombre est-il divisible par 3 ? Réponse : $3 = 0$! Autrement dit, on travaille modulo 3.

Pourquoi ? $10 = 9 + 1 = 3 \times 3 + 1 \equiv 1[3]$.

Exemple

$123456 \equiv 1 + 2 + \cancel{3} + 4 + 5 + \cancel{6}[3] \equiv 1 + 2 + 4 + 5[3] \equiv 0[3]$.

$\rightsquigarrow$ 123456 est divisible par 3.

Exemple

$23456 \equiv 2[3]$: 23456 n'est pas divisible par 3.

Remarque (Preuve par 3)

On peut faire comme pour la preuve par 9. . .mais avec davantage de risque de laisser passer une erreur (pourquoi ?).

• Un nombre est-il divisible par 5 ? $5 = 0$.

$10 \equiv 0[5] \rightsquigarrow$ on retrouve la règle simple : le nombre finit par 0 ou 5.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.

$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.

$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.

$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.

$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11].$

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11].$
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11].$
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11].$
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11].$
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste...modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11].$

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11].$
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11].$
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11].$
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11].$
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Preuve par 11

$10 \equiv -1[11] \Longrightarrow 100 \equiv 1[11]$.

Exemple ($17 \times 35 = 595$)

$17 = 10 + 7 \equiv -1 + 7[11] \equiv 6[11]$.
$35 = 30 + 5 \equiv -3 + 5[11] \equiv 2[11]$.
$17 \times 35 \equiv 6 \times 2[11] \equiv 12[11] \equiv 1[11]$.
$595 = 5 \times 100 + 9 \times 10 + 5 \equiv 5 - 9 + 5[11] \equiv 1[11]$.
$\rightsquigarrow$ on passe le test.

Encore une fois, c'est une indication, pas une preuve. Test complémentaire de la preuve par 9 : si les deux tests sont positifs, alors le calcul est juste. . .modulo une erreur d'un multiple de 99.

Extensions et applications

Cette notion de congruence est à la base de la cryptographie moderne : cartes à puces, connexions sécurisées sur internet, etc.

Théorème (Petit théorème de Fermat)

Si $p \geqslant 2$ est un nombre premier, alors pour tout nombre entier a,

$$a^p \equiv a[p].$$

Si de plus a n'est pas un multiple de p ($a \not\equiv 0[p]$),

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

(Pierre de Fermat : 1601-1655.)

Exemple (RSA : R. Rivest, A. Shamir & L. Adleman, 1977)

Un utilisateur possède une clé publique (deux nombres entiers), ce qui permet aux autres d'envoyer des messages codés.

Extensions et applications

Cette notion de congruence est à la base de la cryptographie moderne : cartes à puces, connexions sécurisées sur internet, etc.

Théorème (Petit théorème de Fermat)

Si $p \geqslant 2$ est un nombre premier, alors pour tout nombre entier a,

$$a^p \equiv a[p].$$

Si de plus a n'est pas un multiple de p ($a \not\equiv 0[p]$),

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

(Pierre de Fermat : 1601-1655.)

Exemple (RSA : R. Rivest, A. Shamir & L. Adleman, 1977)

Un utilisateur possède une clé publique (deux nombres entiers), ce qui permet aux autres d'envoyer des messages codés.

Extensions et applications

Cette notion de congruence est à la base de la cryptographie moderne : cartes à puces, connexions sécurisées sur internet, etc.

Théorème (Petit théorème de Fermat)

Si $p \geqslant 2$ est un nombre premier, alors pour tout nombre entier a,

$$a^p \equiv a[p].$$

Si de plus a n'est pas un multiple de p ($a \not\equiv 0[p]$),

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

(Pierre de Fermat : 1601-1655.)

Exemple (RSA : R. Rivest, A. Shamir & L. Adleman, 1977)

Un utilisateur possède une clé publique (deux nombres entiers), ce qui permet aux autres d'envoyer des messages codés.

Extensions et applications

Cette notion de congruence est à la base de la cryptographie moderne : cartes à puces, connexions sécurisées sur internet, etc.

Théorème (Petit théorème de Fermat)

Si $p \geqslant 2$ est un nombre premier, alors pour tout nombre entier a,

$$a^p \equiv a[p].$$

Si de plus a n'est pas un multiple de p ($a \not\equiv 0[p]$),

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

(Pierre de Fermat : 1601-1655.)

Exemple (RSA : R. Rivest, A. Shamir & L. Adleman, 1977)

Un utilisateur possède une clé publique (deux nombres entiers), ce qui permet aux autres d'envoyer des messages codés.

Cryptographie RSA : cadre mathématique

Rémi veut envoyer un message à Sophie, sous la forme d'un nombre entier M (texte codé par un code ≪ standard ≫).

Sophie génère 4 nombres :

- Deux nombres premiers $p \neq q$.
- Deux nombres c et d tels que $cd \equiv 1[(p-1)(q-1)]$.

La clé publique est le couple (n, c), où $n = p \times q$.

Rémi connait (comme tout le monde) n et c. Il calcule son message chiffré

$$\Sigma \equiv M^c[n].$$

Sophie reçoit Σ, et calcule $\Sigma^d[n]$ (elle seule connait d : clé privée).

Petit théorème de Fermat : $\Sigma^d = M^{cd} \equiv M[n]$

$\Longrightarrow$ Sophie a décodé le message M.

Robustesse : très long de factoriser un grand nombre en facteurs premiers.

Cryptographie RSA : cadre mathématique

Rémi veut envoyer un message à Sophie, sous la forme d'un nombre entier M (texte codé par un code « standard »).
Sophie génère 4 nombres :

- Deux nombres premiers $p \neq q$.
- Deux nombres c et d tels que $cd \equiv 1[(p-1)(q-1)]$.

La clé publique est le couple (n, c), où $n = p \times q$.
Rémi connait (comme tout le monde) n et c. Il calcule son message chiffré

$$\Sigma \equiv M^c[n].$$

Sophie reçoit Σ, et calcule $\Sigma^d[n]$ (elle seule connait d : clé privée).
Petit théorème de Fermat : $\Sigma^d = M^{cd} \equiv M[n]$
$\Longrightarrow$ Sophie a décodé le message M.
Robustesse : très long de factoriser un grand nombre en facteurs premiers.

Cryptographie RSA : cadre mathématique

Rémi veut envoyer un message à Sophie, sous la forme d'un nombre entier M (texte codé par un code « standard »).
Sophie génère 4 nombres :

- Deux nombres premiers $p \neq q$.
- Deux nombres c et d tels que $cd \equiv 1[(p-1)(q-1)]$.

La clé publique est le couple (n, c), où $n = p \times q$.
Rémi connait (comme tout le monde) n et c. Il calcule son message chiffré

$$\Sigma \equiv M^c[n].$$

Sophie reçoit Σ, et calcule $\Sigma^d[n]$ (elle seule connait d : clé privée).
Petit théorème de Fermat : $\Sigma^d = M^{cd} \equiv M[n]$
$\Longrightarrow$ Sophie a décodé le message M.
Robustesse : très long de factoriser un grand nombre en facteurs premiers.

Cryptographie RSA : cadre mathématique

Rémi veut envoyer un message à Sophie, sous la forme d'un nombre entier M (texte codé par un code « standard »).
Sophie génère 4 nombres :

- Deux nombres premiers $p \neq q$.
- Deux nombres c et d tels que $cd \equiv 1[(p-1)(q-1)]$.

La clé publique est le couple (n, c), où $n = p \times q$.
Rémi connait (comme tout le monde) n et c. Il calcule son message chiffré

$$\Sigma \equiv M^c[n].$$

Sophie reçoit Σ, et calcule $\Sigma^d[n]$ (elle seule connait d : clé privée).
Petit théorème de Fermat : $\Sigma^d = M^{cd} \equiv M[n]$
$\Longrightarrow$ Sophie a décodé le message M.
Robustesse : très long de factoriser un grand nombre en facteurs premiers.

Cryptographie RSA : cadre mathématique

Rémi veut envoyer un message à Sophie, sous la forme d'un nombre entier M (texte codé par un code « standard »).
Sophie génère 4 nombres :

- Deux nombres premiers $p \neq q$.
- Deux nombres c et d tels que $cd \equiv 1[(p-1)(q-1)]$.

La clé publique est le couple (n, c), où $n = p \times q$.
Rémi connait (comme tout le monde) n et c. Il calcule son message chiffré

$$\Sigma \equiv M^c[n].$$

Sophie reçoit Σ, et calcule $\Sigma^d[n]$ (elle seule connait d : clé privée).
Petit théorème de Fermat : $\Sigma^d = M^{cd} \equiv M[n]$
$\Longrightarrow$ Sophie a décodé le message M.
Robustesse : très long de factoriser un grand nombre en facteurs premiers.

Cryptographie RSA : cadre mathématique

Rémi veut envoyer un message à Sophie, sous la forme d'un nombre entier M (texte codé par un code « standard »).
Sophie génère 4 nombres :

- Deux nombres premiers $p \neq q$.
- Deux nombres c et d tels que $cd \equiv 1[(p-1)(q-1)]$.

La clé publique est le couple (n, c), où $n = p \times q$.
Rémi connait (comme tout le monde) n et c. Il calcule son message chiffré

$$\Sigma \equiv M^c[n].$$

Sophie reçoit Σ, et calcule $\Sigma^d[n]$ (elle seule connait d : clé privée).
Petit théorème de Fermat : $\Sigma^d = M^{cd} \equiv M[n]$
$\Longrightarrow$ Sophie a décodé le message M.
Robustesse : très long de factoriser un grand nombre en facteurs premiers.

Cryptographie RSA : cadre mathématique

Rémi veut envoyer un message à Sophie, sous la forme d'un nombre entier M (texte codé par un code « standard »).
Sophie génère 4 nombres :

- Deux nombres premiers $p \neq q$.
- Deux nombres c et d tels que $cd \equiv 1[(p-1)(q-1)]$.

La clé publique est le couple (n, c), où $n = p \times q$.
Rémi connait (comme tout le monde) n et c. Il calcule son message chiffré

$$\Sigma \equiv M^c[n].$$

Sophie reçoit Σ, et calcule $\Sigma^d[n]$ (elle seule connait d : clé privée).
Petit théorème de Fermat : $\Sigma^d = M^{cd} \equiv M[n]$
$\Longrightarrow$ Sophie a décodé le message M.
Robustesse : très long de factoriser un grand nombre en facteurs premiers.

Euclide

Les *Éléments* d'Euclide (environ 300 ans avant notre ère) : 13 livres,

- $1-6$: géométrie plane (dont le théorème de Pythagore).
- $7-9$: arithmétique (dont la division euclidienne).
- 10 : nombres irrationnels ($\sqrt{2}$, etc.)
- $11-13$: géométrie dans l'espace.

$\rightsquigarrow$ livre de référence pendant plus de 2000 ans (recherche et enseignement).
Géométrie plane : 5 postulats.

Euclide

Les *Éléments* d'Euclide (environ 300 ans avant notre ère) : 13 livres,

- $1-6$: géométrie plane (dont le théorème de Pythagore).
- $7-9$: arithmétique (dont la division euclidienne).
- 10 : nombres irrationnels ($\sqrt{2}$, etc.)
- $11-13$: géométrie dans l'espace.

$\rightsquigarrow$ livre de référence pendant plus de 2000 ans (recherche et enseignement).

Géométrie plane : 5 postulats.

Euclide

Les *Éléments* d'Euclide (environ 300 ans avant notre ère) : 13 livres,

- $1-6$: géométrie plane (dont le théorème de Pythagore).
- $7-9$: arithmétique (dont la division euclidienne).
- 10 : nombres irrationnels ($\sqrt{2}$, etc.)
- $11-13$: géométrie dans l'espace.

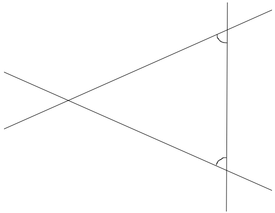
$\rightsquigarrow$ livre de référence pendant plus de 2000 ans
(recherche et enseignement).
Géométrie plane : 5 postulats.

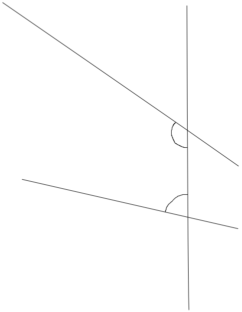
Géométrie euclidienne

1. Un segment de droite peut être tracé en joignant deux points quelconques.
2. Un segment de droite peut être prolongé indéfiniment en une ligne droite.
3. Étant donné un segment de droite quelconque, un cercle peut être tracé en prenant ce segment comme rayon et l'une de ses extrémités comme centre.
4. Tous les angles droits sont congruents.
5. Si deux lignes sont sécantes avec une troisième de telle façon que la somme des angles intérieurs d'un côté est inférieure à deux angles droits, alors ces deux lignes sont forcément sécantes de ce côté.

Le 5^{e} postulat d'Euclide

5. Si deux lignes sont sécantes avec une troisième de telle façon que la somme des angles intérieurs d'un côté est inférieure à deux angles droits, alors ces deux lignes sont forcément sécantes de ce côté.





Le 5^{e} postulat revisité

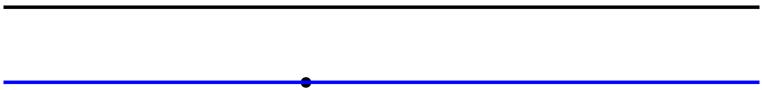
Par Proclus :

5. Par un point donné hors d'une droite, on peut mener une et une seule parallèle à cette droite.

Le 5^{e} postulat revisité

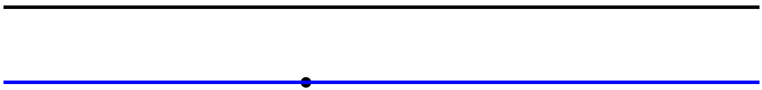
Par Proclus :

5. Par un point donné hors d'une droite, on peut mener une et une seule parallèle à cette droite.



Par Proclus :

5. Par un point donné hors d'une droite, on peut mener une et une seule parallèle à cette droite.



Par Khayyam :

5. La somme des angles d'un triangle est égale à 180°.

On garde les quatre premiers postulats, mais on « joue » avec le 5^{e} :

> *Par un point donné hors d'une droite, combien peut-on mener de parallèle à cette droite ?*

Géométries non euclidiennes

On garde les quatre premiers postulats, mais on « joue » avec le 5^{e} :

> *Par un point donné hors d'une droite, combien peut-on mener de parallèle à cette droite ?*

On garde les quatre premiers postulats, mais on ≪ joue ≫ avec le 5e :

Par un point donné hors d'une droite, combien peut-on mener de parallèle à cette droite ?

- Une et une seule : géométrie euclidienne.

Géométries non euclidiennes

On garde les quatre premiers postulats, mais on « joue » avec le 5e :

Par un point donné hors d'une droite, combien peut-on mener de parallèle à cette droite ?

- Une et une seule : géométrie euclidienne.
- Aucune : géométrie sphérique.

Géométries non euclidiennes

On garde les quatre premiers postulats, mais on « joue » avec le 5^{e} :

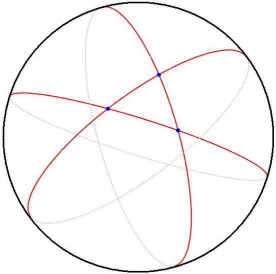
> *Par un point donné hors d'une droite, combien peut-on mener de parallèle à cette droite ?*

- Une et une seule : géométrie euclidienne.
- Aucune : géométrie sphérique.
- Une infinité : géométrie hyperbolique.

Géométrie sphérique

Par un point donné hors d'une droite, on ne peut mener aucune parallèle à cette droite

Absurde. . .et pourtant : sur une sphère ($\approx$ la Terre), les droites (les plus courts chemins d'un point à un autre, localement) sont des grands cercles :

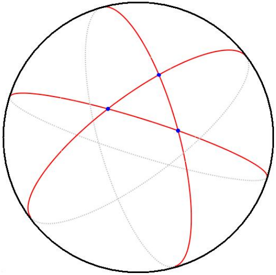


Les grands cercles d'une sphère se coupent tous !

Il n'existe pas de droites parallèles non confondues.

Par un point donné hors d'une droite, on ne peut mener aucune parallèle à cette droite

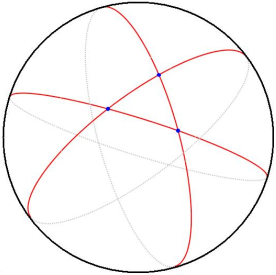
Absurde. . .et pourtant : sur une sphère (≈ la Terre), les droites (les plus courts chemins d'un point à un autre, localement) sont des grands cercles :



Les grands cercles d'une sphère se coupent tous !
Il n'existe pas de droites parallèles non confondues.

Par un point donné hors d'une droite, on ne peut mener aucune parallèle à cette droite

Absurde...et pourtant : sur une sphère ($\approx$ la Terre), les droites (les plus courts chemins d'un point à un autre, localement) sont des grands cercles :

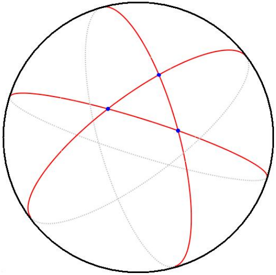


Les grands cercles d'une sphère se coupent tous !
Il n'existe pas de droites parallèles non confondues.

Géométrie sphérique

Par un point donné hors d'une droite, on ne peut mener aucune parallèle à cette droite

Absurde. . .et pourtant : sur une sphère ($\approx$ la Terre), les droites (les plus courts chemins d'un point à un autre, localement) sont des grands cercles :



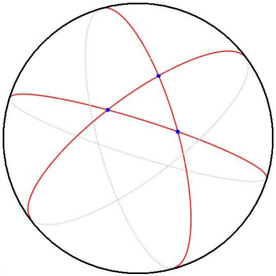
Les grands cercles d'une sphère se coupent tous !

Il n'existe pas de droites parallèles non confondues.

Géométrie sphérique

Par un point donné hors d'une droite, on ne peut mener aucune parallèle à cette droite

Absurde. . .et pourtant : sur une sphère ($\approx$ la Terre), les droites (les plus courts chemins d'un point à un autre, localement) sont des grands cercles :



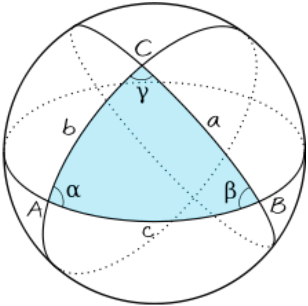
Les grands cercles d'une sphère se coupent tous !
Il n'existe pas de droites parallèles non confondues.

Par l'approche de Khayyam :

La somme des angles d'un triangle est supérieure à 180^o.

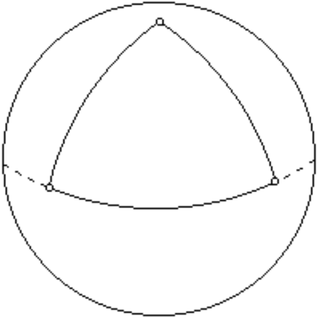
Par l'approche de Khayyam :

La somme des angles d'un triangle est supérieure à 180°.



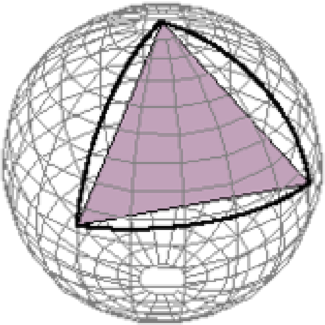
Par l'approche de Khayyam :

La somme des angles d'un triangle est supérieure à 180°.



Par l'approche de Khayyam :

La somme des angles d'un triangle est supérieure à 180°.



La géométrie hyperbolique

Par un point donné hors d'une droite, on peut mener une infinité de parallèles à cette droite

Ou encore :

La somme des angles d'un triangle est inférieure à 180°.

La géométrie hyperbolique

> *Par un point donné hors d'une droite, on peut mener une infinité de parallèles à cette droite*

Ou encore :

> *La somme des angles d'un triangle est inférieure à* 180^o*.*

La géométrie hyperbolique

Par un point donné hors d'une droite, on peut mener une infinité de parallèles à cette droite

Ou encore :

La somme des angles d'un triangle est inférieure à 180°.

Notion développée par Henri Poincaré (1854-1912).

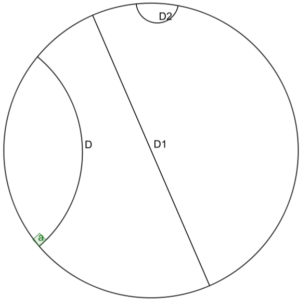
Le disque de Poincaré

Supposons (. . .) un monde renfermé dans [un grand cercle] et soumis aux lois suivantes :
La température n'est pas uniforme ; elle est maxima au centre, et elle diminue à mesure qu'on s'en éloigne, pour se réduire au zéro absolu quand on atteint [le cercle] où ce monde est renfermé.
(. . .) Si ce monde est limité au point de vue de notre géométrie habituelle, il paraîtra infini à ses habitants. Quand ceux-ci, en effet, veulent se rapprocher [du cercle], ils se refroidissent et deviennent de plus en plus petits. Les pas qu'ils font sont de plus en plus petits, de sorte qu'ils ne peuvent jamais atteindre [le cercle].

Le monde hyperbolique

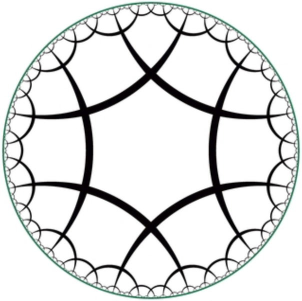
Les droites sont des arcs de cercles qui coupent le cercle à angle droit, et les diamètres du cercle :

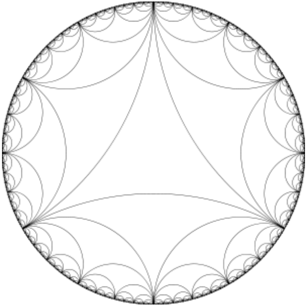
Les droites sont des arcs de cercles qui coupent le cercle à angle droit, et les diamètres du cercle :



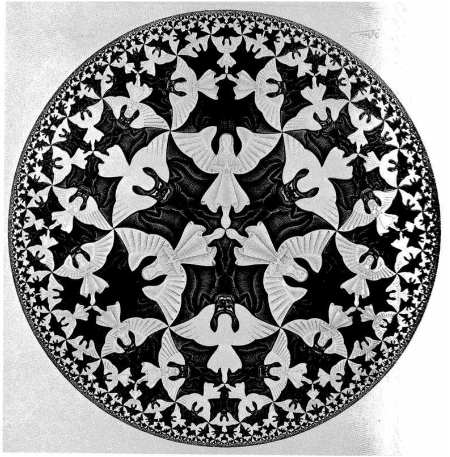
Le monde hyperbolique

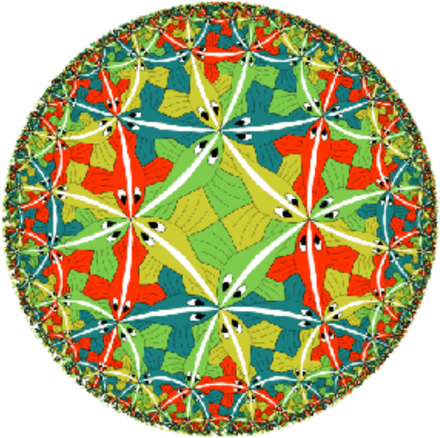
Les droites sont des arcs de cercles qui coupent le cercle à angle droit, et les diamètres du cercle :





Le disque de Poincaré selon M. C. Escher





Et pourtant, ça sert

L'introduction de la géométrie non euclidienne est une caractéristique forte qui distingue la physique selon Newton de la physique selon Einstein.

La théorie de la relativité générale est une théorie géométrique, qui génère encore aujourd'hui de la recherche en mathématique (notion d'espace-temps courbe).

Avec Newton uniquement, les GPS ne fonctionneraient pas : on a besoin des corrections apportées par Einstein.

Et pourtant, ça sert

L'introduction de la géométrie non euclidienne est une caractéristique forte qui distingue la physique selon Newton de la physique selon Einstein.

La théorie de la relativité générale est une théorie géométrique, qui génère encore aujourd'hui de la recherche en mathématique (notion d'espace-temps courbe).

Avec Newton uniquement, les GPS ne fonctionneraient pas : on a besoin des corrections apportées par Einstein.

Et pourtant, ça sert

L'introduction de la géométrie non euclidienne est une caractéristique forte qui distingue la physique selon Newton de la physique selon Einstein.
La théorie de la relativité générale est une théorie géométrique, qui génère encore aujourd'hui de la recherche en mathématique (notion d'espace-temps courbe).
Avec Newton uniquement, les GPS ne fonctionneraient pas : on a besoin des corrections apportées par Einstein.

Écoutons Poincaré

Le savant digne de ce nom, le géomètre surtout, éprouve en face de son œuvre la même impression que l'artiste ; sa jouissance est aussi grande et de même nature. Si je n'écrivais pas pour un public amoureux de la Science, je n'oserais pas m'exprimer ainsi : je redouterais l'incrédulité des profanes. Mais ici, je puis dire toute ma pensée. Si nous travaillons, c'est moins pour obtenir ces résultats positifs auxquels le vulgaire nous croit uniquement attachés, que pour ressentir cette émotion esthétique et la communiquer à ceux qui sont capables de l'éprouver.

Pour aller plus loin sur internet

Site Images des mathématiques du CNRS :

http://images.math.cnrs.fr/

Deux films réalisés en France :

- Dimensions : http://www.dimensions-math.org/
- Chaos : http://www.chaos-math.org/

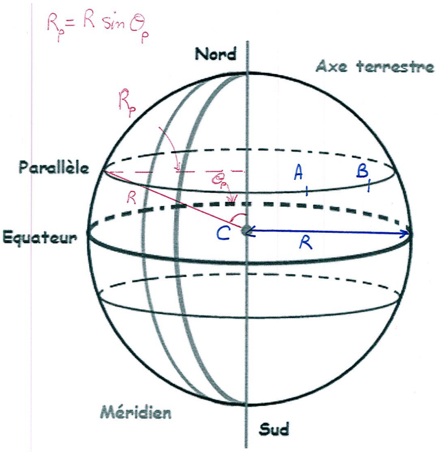
Pour aller plus loin sur internet

Site Images des mathématiques du CNRS :

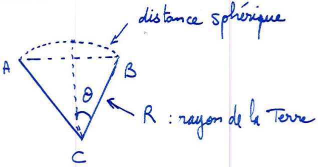
http://images.math.cnrs.fr/

Deux films réalisés en France :

- Dimensions : http://www.dimensions-math.org/
- Chaos : http://www.chaos-math.org/



Plan ABC

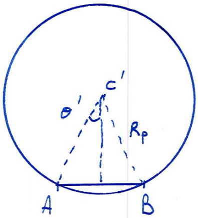


$$d_{\text{espace}}(A,B) = 2R\sin\theta$$

$$d_{\text{sphérique}}(A,B) = 2R\theta$$

On a toujours : $\theta \geqslant \sin\theta$

Plan du parallèle



R_p : rayon du parallèle

$R_p = R \sin \theta_p$

$$\sin \theta' = \frac{R \sin \theta}{R_p} = \frac{\sin \theta}{\sin \theta_p} \geq \sin \theta$$

$$\Rightarrow \boxed{\theta' \geq \theta}$$

Or $d_{\text{parallèle}}(A,B) = 2 R_p \theta' = 2 R \theta' \sin \theta_p$

$$= \underbrace{2R\theta}_{d_{\text{spérique}}(A,B)} \underbrace{\frac{\sin\theta}{\theta} \frac{\theta'}{\sin \theta'}}_{\geq 1 \text{ car } \theta' \geq \theta}$$

et $x \longmapsto \dfrac{\sin x}{x}$

décroissante sur $[0, \frac{\pi}{2}]$.