ARITHMÉTIQUE I
Division - Congruences - PGCD

Guillaume CONNAN

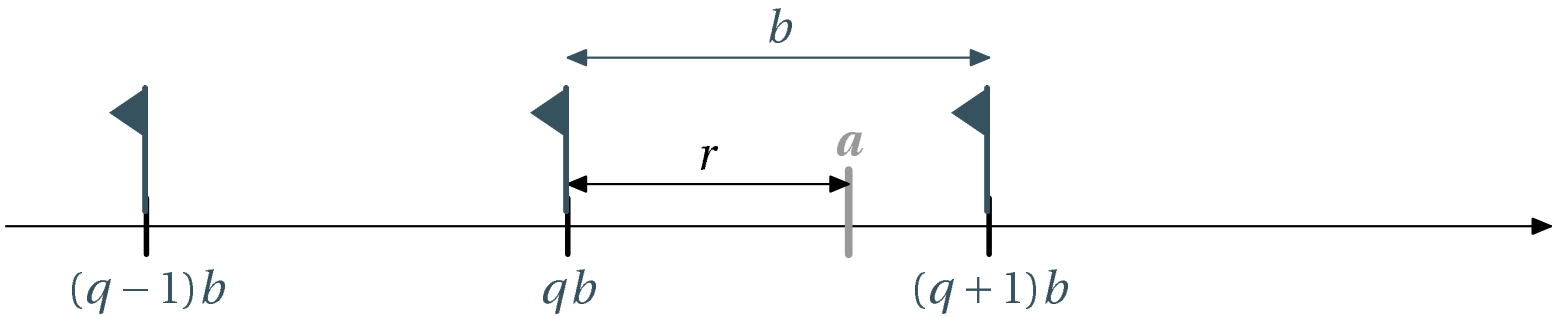
Lycée Jean PERRIN

Septembre 2006

Sommaire

Sommaire

Le dessin 4



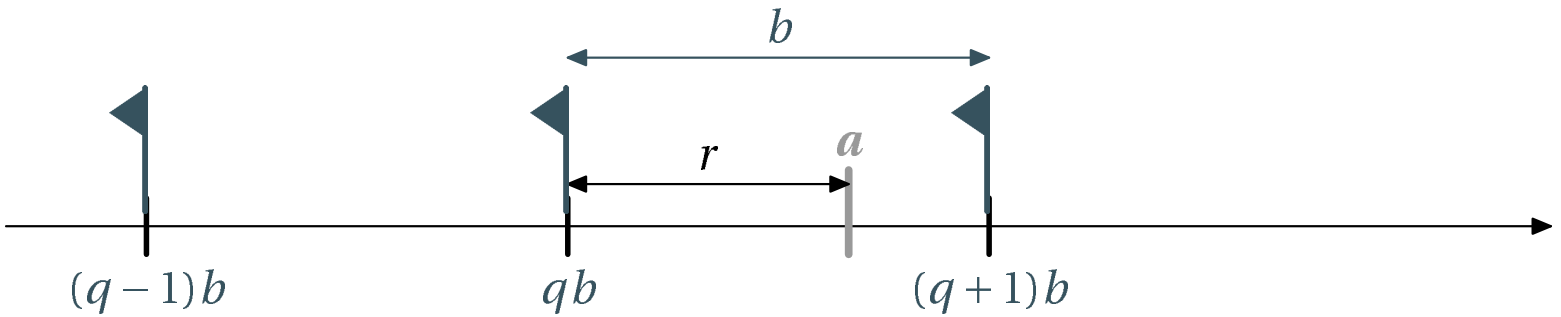
Théorème

- *Soit a un entier relatif et b un entier naturel non nul.*
- *Il existe un unique couple d'entiers $(q;r)$ tels que*

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

- *Déterminer q et r, c'est effectuer la division euclidienne de a par b.*
- *On appelle a le dividende, b le diviseur, q le quotient et r le reste.*

Le dessin 4



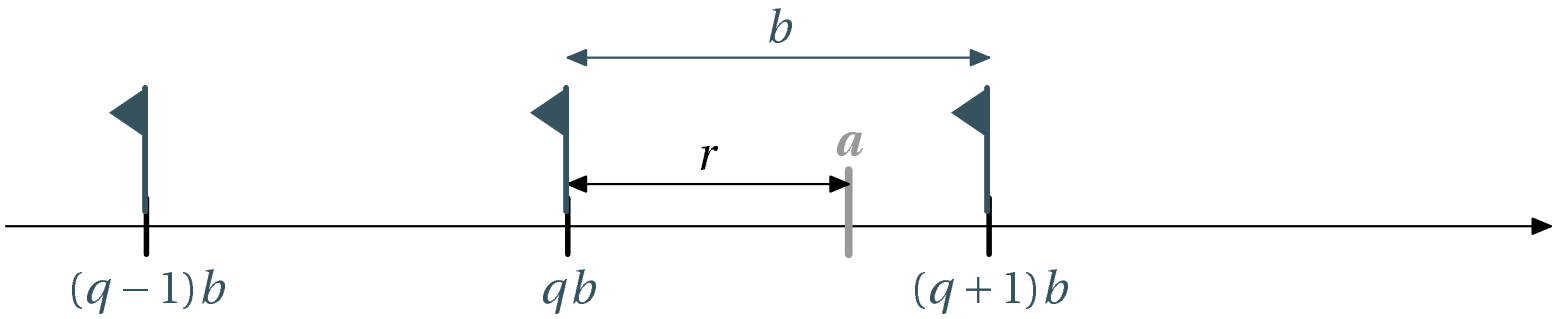
Théorème

- *Soit a un entier relatif et b un entier naturel non nul*
- *Il existe un unique couple d'entiers (q; r) tels que*

$$a = bq + r \text{ avec } 0 \leq r < b$$

- *Déterminer q et r, c'est effectuer la division euclidienne de a par b.*
- *On appelle a le dividende, b le diviseur, q le quotient et r le reste.*

Le dessin 4



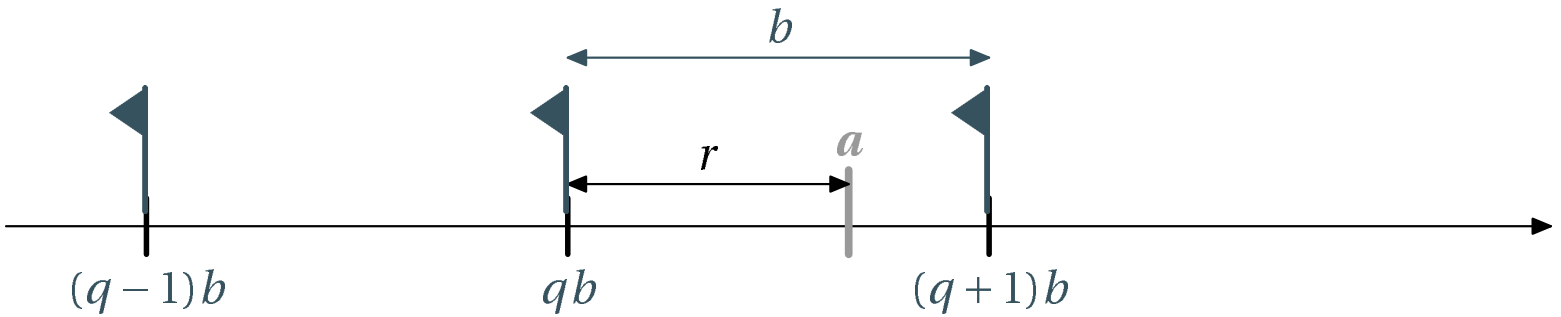
Théorème

- *Soit a un entier relatif et b un entier naturel non nul.*
- *Il existe un unique couple d'entiers (q, r) tels que*

$$a = bq + r \quad avec \quad 0 \leqslant r < b$$

- *Déterminer q et r, c'est effectuer la division euclidienne de a par b.*
- *On appelle a le dividende, b le diviseur, q le quotient et r le reste.*

Le dessin 4



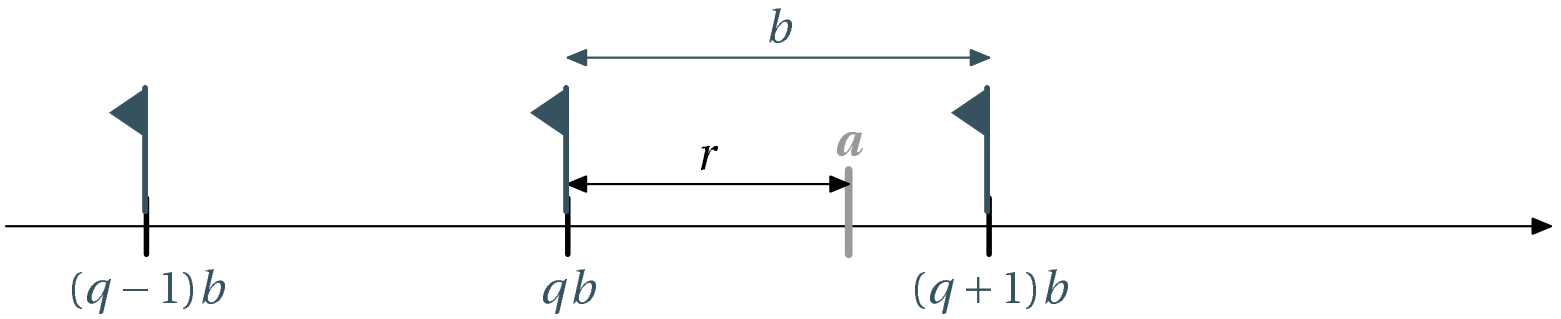
Théorème

- *Soit a un entier relatif et b un entier naturel non nul.*
- *Il existe un unique couple d'entiers (q, r) tels que*

$$a = bq + r \quad avec \quad 0 \leqslant r < b$$

- *Déterminer q et r, c'est effectuer la division euclidienne de a par b.*
- *On appelle a le dividende, b le diviseur, q le quotient et r le reste.*

Le dessin 4



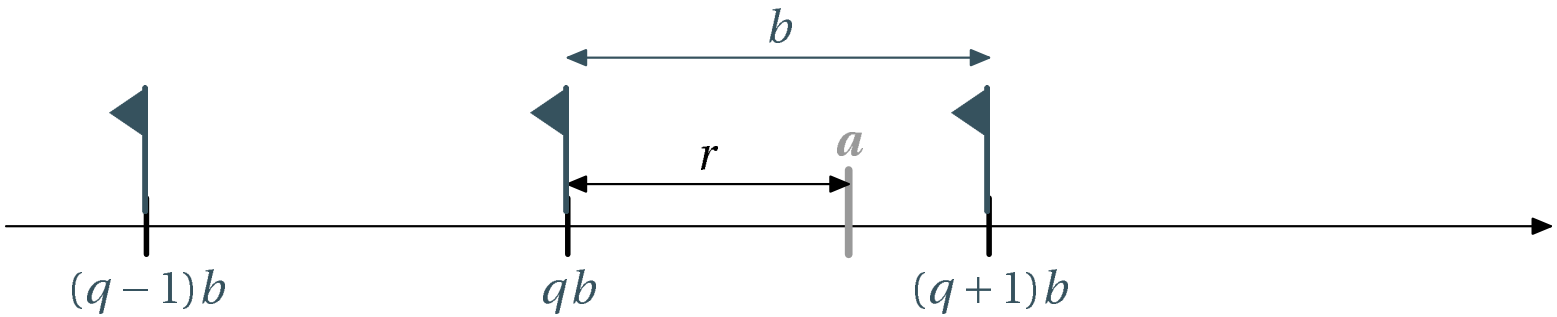
Théorème

- *Soit a un entier relatif et b un entier naturel non nul.*
- *Il existe un unique couple d'entiers (q, r) tels que*

$$a = bq + r \quad avec \quad 0 \leqslant r < b$$

- *Déterminer q et r, c'est effectuer la division euclidienne de a par b.*
- *On appelle a le dividende, b le diviseur, q le quotient et r le reste.*

Le dessin 4



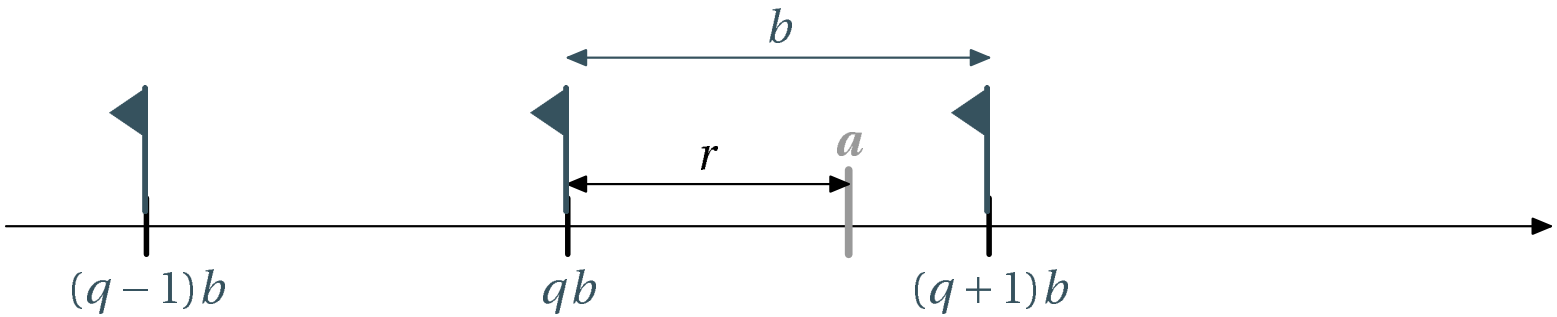
Théorème

- *Soit a un entier relatif et b un entier naturel non nul.*
- *Il existe un unique couple d'entiers (q, r) tels que*

$$a = bq + r \quad avec \quad 0 \leqslant r < b$$

- *Déterminer q et r, c'est effectuer la division euclidienne de a par b.*
- *On appelle a le dividende, b le diviseur, q le quotient et r le reste.*

Le dessin 4



Théorème

- *Soit a un entier relatif et b un entier naturel non nul.*
- *Il existe un unique couple d'entiers (q, r) tels que*

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

- *Déterminer q et r, c'est effectuer la division euclidienne de a par b.*
- *On appelle a le dividende, b le diviseur, q le quotient et r le reste.*

Sommaire

Le dessin est le secret de la démonstration
Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Le dessin est le secret de la démonstration

Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Le dessin est le secret de la démonstration
Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Le dessin est le secret de la démonstration
Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Le dessin est le secret de la démonstration
Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Le dessin est le secret de la démonstration
Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Le dessin est le secret de la démonstration
Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Le dessin est le secret de la démonstration
Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Le dessin est le secret de la démonstration
Il traduit qu'un entier a est

- soit un multiple de b
- soit est encadré par deux multiples consécutifs de b

Il faudra prouver

- qu'un tel couple existe
- qu'il est unique

Existence

Nous traiterons le cas où $a \in \mathbb{N}$
Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?
Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Existence

Nous traiterons le cas où $a \in \mathbb{N}$

Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?
Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Existence

Nous traiterons le cas où $a \in \mathbb{N}$
Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?
Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Existence

Nous traiterons le cas où $a \in \mathbb{N}$
Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?
Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Existence

Nous traiterons le cas où $a \in \mathbb{N}$
Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?
Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Existence

Nous traiterons le cas où $a \in \mathbb{N}$
Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?
Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Existence

Nous traiterons le cas où $a \in \mathbb{N}$
Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?

Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Existence

Nous traiterons le cas où $a \in \mathbb{N}$
Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?
Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Existence

Nous traiterons le cas où $a \in \mathbb{N}$
Soit $\mathscr{M}_i$ l'ensemble des multiples de b inférieurs ou égaux à a.

- $\mathscr{M}_i$ est non vide car ...
- $\mathscr{M}_i$ est majoré par ...

L'ensemble $\mathscr{M}_i$ est donc une partie de $\mathbb{N}$ non vide et majorée : conclusion ?
Appelons μ ce plus grand élément.
Comment peut-on écrire μ en fonction de b ?

Unicité : suite

C'est un multiple de b, donc il existe un entier q tel que $\mu = qb$.
Que dire du multiple suivant de b ?
On en déduit que

$$bq \leqslant a < bq + b$$

Regardons à nouveau le dessin 2 : comment introduie le reste ?
Nous avons donc démontré l'existence de deux entiers q et r tels que $a = bq + r$ avec $0 \leqslant r < b$

Unicité : suite

C'est un multiple de b, donc il existe un entier q tel que $\mu = qb$.

Que dire du multiple suivant de b ?

On en déduit que

$$bq \leqslant a < bq + b$$

Regardons à nouveau le dessin 2 : comment introduie le reste ?

Nous avons donc démontré l'existence de deux entiers q et r tels que $a = bq + r$ avec $0 \leqslant r < b$

Unicité : suite

C'est un multiple de b, donc il existe un entier q tel que $\mu = qb$.
Que dire du multiple suivant de b ?
On en déduit que

$$bq \leqslant a < bq + b$$

Regardons à nouveau le dessin 2 : comment introduie le reste ?
Nous avons donc démontré l'existence de deux entiers q et r tels que $a = bq + r$ avec $0 \leqslant r < b$

Unicité : suite

C'est un multiple de b, donc il existe un entier q tel que $\mu = qb$.
Que dire du multiple suivant de b ?
On en déduit que

$$bq \leqslant a < bq + b$$

Regardons à nouveau le dessin 2 : comment introduie le reste ?
Nous avons donc démontré l'existence de deux entiers q et r tels que $a = bq + r$ avec $0 \leqslant r < b$

Unicité : suite

C'est un multiple de b, donc il existe un entier q tel que $\mu = qb$.
Que dire du multiple suivant de b ?
On en déduit que

$$bq \leqslant a < bq + b$$

Regardons à nouveau le dessin 2 : comment introduie le reste ?
Nous avons donc démontré l'existence de deux entiers q et r tels que $a = bq + r$ avec $0 \leqslant r < b$

Unicité : suite

C'est un multiple de b, donc il existe un entier q tel que $\mu = qb$.
Que dire du multiple suivant de b ?
On en déduit que

$$bq \leqslant a < bq + b$$

Regardons à nouveau le dessin 2 : comment introduie le reste ?
Nous avons donc démontré l'existence de deux entiers q et r tels que $a = bq + r$ avec $0 \leqslant r < b$

Unicité

Supposons qu'il existe deux couples et montrons que c'est impossible.

- $a = bq + r$ avec $0 \leqslant r < b$
- $a = bq' + r'$ avec $0 \leqslant r' < b$

Effectuez la différence membre à membre de ces égalités.
Que dire de $r - r'$?

Unicité

Supposons qu'il existe deux couples et montrons que c'est impossible.

- $a = bq + r$ avec $0 \leqslant r < b$
- $a = bq' + r'$ avec $0 \leqslant r' < b$

Effectuez la différence membre à membre de ces égalités.
Que dire de $r - r'$?

Unicité

Supposons qu'il existe deux couples et montrons que c'est impossible.

- $a = bq + r \quad$ avec $\quad 0 \leqslant r < b$
- $a = bq' + r' \quad$ avec $\quad 0 \leqslant r' < b$

Effectuez la différence membre à membre de ces égalités.
Que dire de $r - r'$?

Unicité

Supposons qu'il existe deux couples et montrons que c'est impossible.

- $a = bq + r \quad$ avec $\quad 0 \leqslant r < b$
- $a = bq' + r' \quad$ avec $\quad 0 \leqslant r' < b$

Effectuez la différence membre à membre de ces égalités.
Que dire de $r - r'$?

Unicité

Supposons qu'il existe deux couples et montrons que c'est impossible.

- $a = bq + r \quad$ avec $\quad 0 \leqslant r < b$
- $a = bq' + r' \quad$ avec $\quad 0 \leqslant r' < b$

Effectuez la différence membre à membre de ces égalités.
Que dire de $r - r'$?

Unicité

Supposons qu'il existe deux couples et montrons que c'est impossible.

- $a = bq + r \quad$ avec $\quad 0 \leqslant r < b$
- $a = bq' + r' \quad$ avec $\quad 0 \leqslant r' < b$

Effectuez la différence membre à membre de ces égalités.
Que dire de $r - r'$?

Unicité

Supposons qu'il existe deux couples et montrons que c'est impossible.

- $a = bq + r \quad$ avec $\quad 0 \leqslant r < b$
- $a = bq' + r' \quad$ avec $\quad 0 \leqslant r' < b$

Effectuez la différence membre à membre de ces égalités. Que dire de $r - r'$?

Sommaire

Calcul du quotient

```
quotient(a,b):={
local k
while(k*b<=a){k:=k+1;}
k-1;
}
```

Calcul du quotient

```
quotient(a,b):={
local k
while(k*b<=a){k:=k+1;}
k-1;
}
```

Calcul du quotient

```
quotient(a,b):={
local k
while(k*b<=a){k:=k+1;}
k-1;
}
```

Calcul du quotient

```
quotient(a,b):={
local k
while(k*b<=a){k:=k+1;}
k-1;
}
```

Calcul du quotient

```
quotient(a,b):={
local k
while(k*b<=a){k:=k+1;}
k-1;
}
```

Calcul du quotient

```
quotient(a,b):={
local k
while(k*b<=a){k:=k+1;}
k-1;
}
```

Calcul du reste

```
reste(a,b):={
local k
while(k*b<=a){k:=k+1;}
-b*(k-1);
}
```

Calcul du reste

```
reste(a,b):={
local k
while(k*b<=a){k:=k+1;}
-b*(k-1);
}
```

Calcul du reste

```
reste(a,b):={
local k
while(k*b<=a){k:=k+1;}
-b*(k-1);
}
```

Calcul du reste

```
reste(a,b):={
local k
while(k*b<=a){k:=k+1;}
-b*(k-1);
}
```

Calcul du reste

```
reste(a,b):={
local k
while(k*b<=a){k:=k+1;}
-b*(k-1);
}
```

Calcul du reste

```
reste(a,b):={
local k
while(k*b<=a){k:=k+1;}
-b*(k-1);
}
```

Sachez tout de même que ces fonctions sont pré-programmées de manière plus efficace sur XCAS

- `iquo(2354,67);`
- `irem(2354,67);`

Sachez tout de même que ces fonctions sont pré-programmées de manière plus efficace sur XCAS

- `iquo(2354,67);`
- `irem(2354,67);`

Sachez tout de même que ces fonctions sont pré-programmées de manière plus efficace sur XCAS

- `iquo(2354,67);`
- `irem(2354,67);`

Sachez tout de même que ces fonctions sont pré-programmées de manière plus efficace sur XCAS

- `iquo(2354,67);`
- `irem(2354,67);`

Sommaire

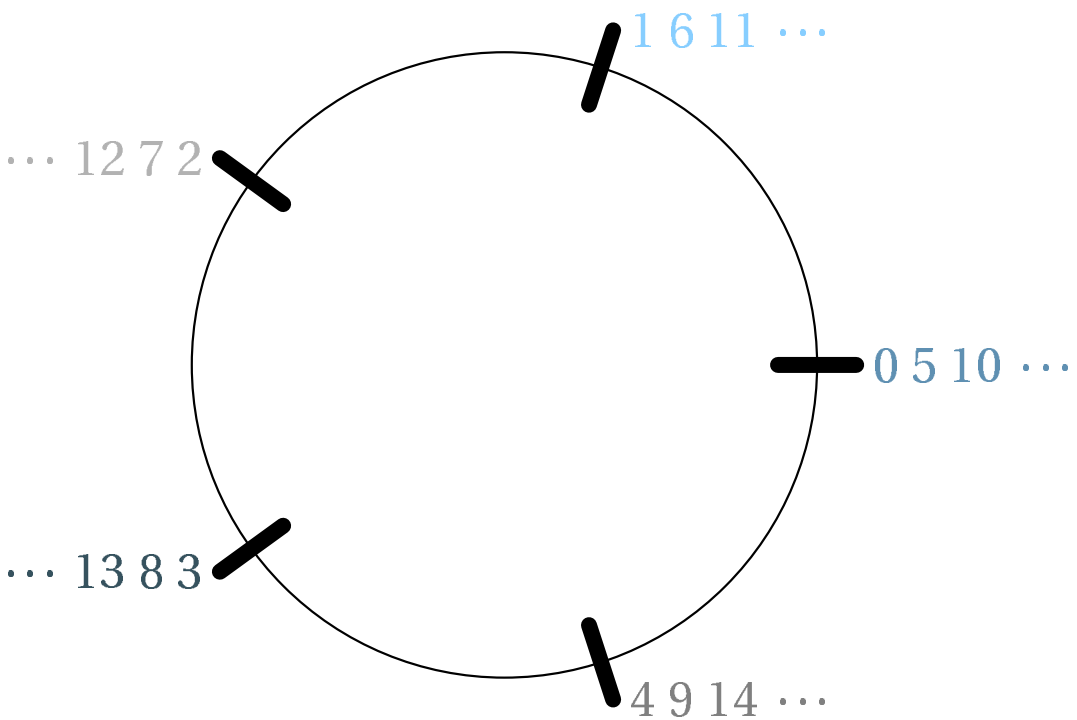
Voici un classement des entiers naturels

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	...			

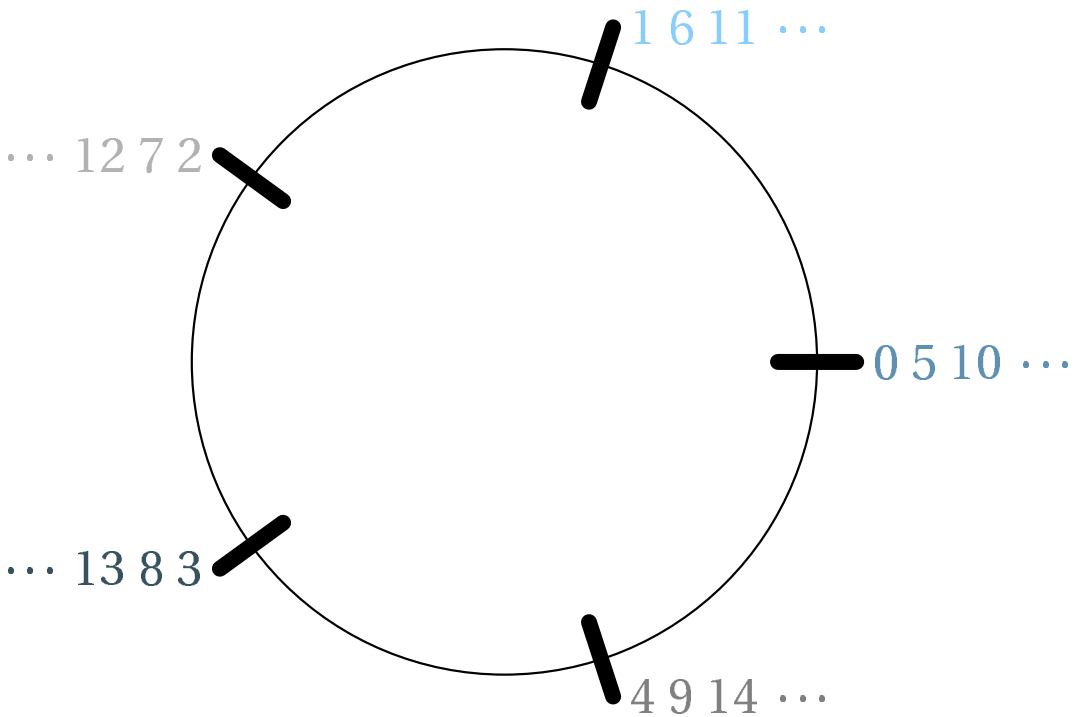
Voici un classement des entiers naturels

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	...			

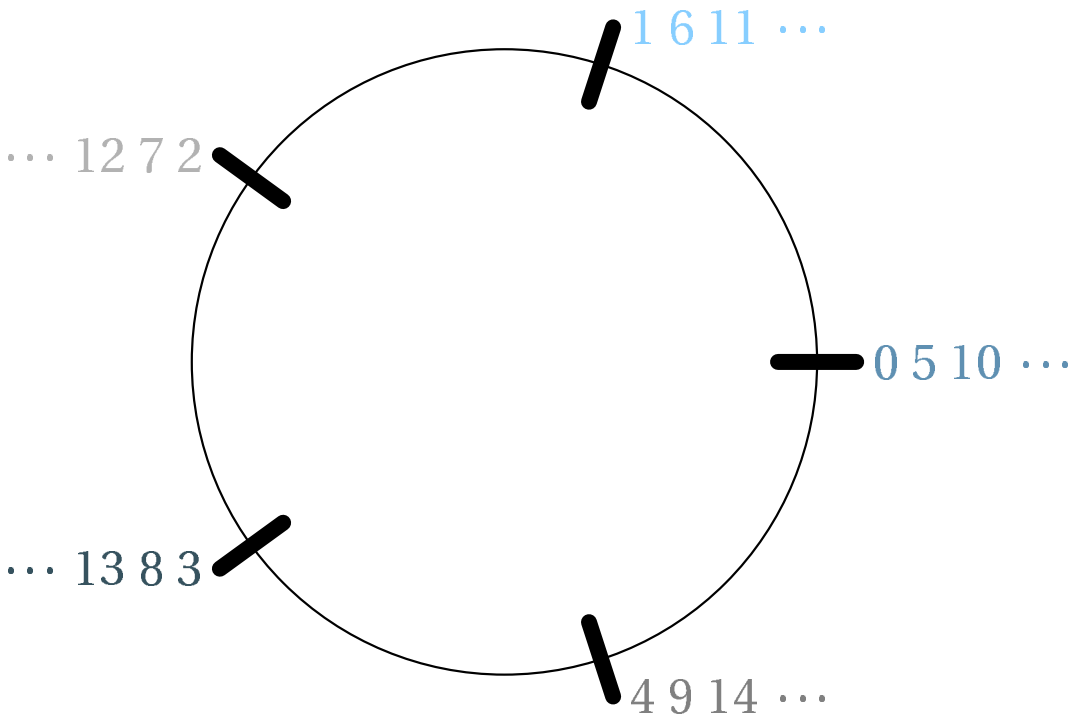
Vous pouvez aussi enrouler la droite des réels graduée par les entiers sur un cercle de périmètre 5 et retrouver les mêmes sensations qu'avec la congruence modulo 2π :



Vous pouvez aussi enrouler la droite des réels graduée par les entiers sur un cercle de périmètre 5 et retrouver les mêmes sensations qu'avec la congruence modulo 2π :



Vous pouvez aussi enrouler la droite des réels graduée par les entiers sur un cercle de périmètre 5 et retrouver les mêmes sensations qu'avec la congruence modulo 2π :



Cela nous permet de classer les entiers par équipes : l'équipe de ceux qui ont pour reste 0 dans la division euclidienne par 5, l'équipe de ceux qui ont pour reste 1, etc.
Maintenant, si Roger, Bébert et Josette font partie de la même équipe, on pourra désigner cette équipe par « équipe de Roger » ou « équipe de Bébert » ou bien « équipe de Josette ».
Pour nos nombres, l'équipe de ceux qui ont pour reste 3 pourra s'appeler l'équipe de 3 ou l'équipe de 8 ou l'équipe de 32318.

Cela nous permet de classer les entiers par équipes : l'équipe de ceux qui ont pour reste 0 dans la division euclidienne par 5, l'équipe de ceux qui ont pour reste 1, etc.

Maintenant, si Roger, Bébert et Josette font partie de la même équipe, on pourra désigner cette équipe par « équipe de Roger » ou « équipe de Bébert » ou bien « équipe de Josette ».

Pour nos nombres, l'équipe de ceux qui ont pour reste 3 pourra s'appeler l'équipe de 3 ou l'équipe de 8 ou l'équipe de 32318.

Cela nous permet de classer les entiers par équipes : l'équipe de ceux qui ont pour reste 0 dans la division euclidienne par 5, l'équipe de ceux qui ont pour reste 1, etc.
Maintenant, si Roger, Bébert et Josette font partie de la même équipe, on pourra désigner cette équipe par « équipe de Roger » ou « équipe de Bébert » ou bien « équipe de Josette ».
Pour nos nombres, l'équipe de ceux qui ont pour reste 3 pourra s'appeler l'équipe de 3 ou l'équipe de 8 ou l'équipe de 32318.

Cela nous permet de classer les entiers par équipes : l'équipe de ceux qui ont pour reste 0 dans la division euclidienne par 5, l'équipe de ceux qui ont pour reste 1, etc.
Maintenant, si Roger, Bébert et Josette font partie de la même équipe, on pourra désigner cette équipe par « équipe de Roger » ou « équipe de Bébert » ou bien « équipe de Josette ».
Pour nos nombres, l'équipe de ceux qui ont pour reste 3 pourra s'appeler l'équipe de 3 ou l'équipe de 8 ou l'équipe de 32318.

Sommaire

Nous venons de dire que nous allons regrouper les nombres selon leur reste dans la division euclidienne par un entier naturel n quelconque cette fois-ci. Il faut donc définir un code pour se reconnaître entre gens du même monde :

Définition

- Soient a et b deux entiers et n un entier naturel supérieur à 2.
- Dire que a est congru à b modulo n signifie que a et b ont le même reste dans la division euclidienne par n.
- On note :

$$a \equiv b [n]$$

Nous venons de dire que nous allons regrouper les nombres selon leur reste dans la division euclidienne par un entier naturel n quelconque cette fois-ci. Il faut donc définir un code pour se reconnaître entre gens du même monde :

Définition

- Soient a et b deux entiers et n un entier naturel supérieur à 2.
- Dire que a est congru à b modulo n signifie que a et b ont le même reste dans la division euclidienne par n.
- On note :

$$a \equiv b [n]$$

Nous venons de dire que nous allons regrouper les nombres selon leur reste dans la division euclidienne par un entier naturel n quelconque cette fois-ci. Il faut donc définir un code pour se reconnaître entre gens du même monde :

Définition

- Soient a et b deux entiers et n un entier naturel supérieur à 2.
- Dire que a est congru à b modulo n signifie que a et b ont le même reste dans la division euclidienne par n.
- On note

$$a \equiv b[n]$$

Nous venons de dire que nous allons regrouper les nombres selon leur reste dans la division euclidienne par un entier naturel n quelconque cette fois-ci. Il faut donc définir un code pour se reconnaître entre gens du même monde :

Définition

- Soient a et b deux entiers et n un entier naturel supérieur à 2.
- Dire que a est congru à b modulo n signifie que a et b ont le même reste dans la division euclidienne par n.
- On note

$$a \equiv b[n]$$

Nous venons de dire que nous allons regrouper les nombres selon leur reste dans la division euclidienne par un entier naturel n quelconque cette fois-ci. Il faut donc définir un code pour se reconnaître entre gens du même monde :

Définition

- Soient a et b deux entiers et n un entier naturel supérieur à 2.
- Dire que a est congru à b modulo n signifie que a et b ont le même reste dans la division euclidienne par n.
- On note

$$a \equiv b[n]$$

Nous venons de dire que nous allons regrouper les nombres selon leur reste dans la division euclidienne par un entier naturel n quelconque cette fois-ci. Il faut donc définir un code pour se reconnaître entre gens du même monde :

Définition

- Soient a et b deux entiers et n un entier naturel supérieur à 2.
- Dire que a est congru à b modulo n signifie que a et b ont le même reste dans la division euclidienne par n.
- On note

$$a \equiv b[n]$$

Sommaire

Propriété fondamentale

Propriété

Soit a et b deux entiers et n un entier naturel.
a est congru à b modulo n si et seulement si a – b est un multiple de n

Preuve

Puisque les congruences sont liés au reste, il faut utiliser les divisions euclidiennes par n.
Je pose donc $a = nq + r$ et $b = nq' + r'$ sans oublier que r et r' sont dans $[\![0, n[\![$.
Que peut-on dire de r et r' ?

Preuve

Puisque les congruences sont liés au reste, il faut utiliser les divisions euclidiennes par n.

Je pose donc $a = nq + r$ et $b = nq' + r'$ sans oublier que r et r' sont dans $[\![0, n[\![$.

Que peut-on dire de r et r' ?

Preuve

Puisque les congruences sont liés au reste, il faut utiliser les divisions euclidiennes par n.
Je pose donc $a = nq + r$ et $b = nq' + r'$ sans oublier que r et r' sont dans $[\![0, n[\![$.
Que peut-on dire de r et r' ?

Preuve

Puisque les congruences sont liés au reste, il faut utiliser les divisions euclidiennes par n.
Je pose donc $a = nq + r$ et $b = nq' + r'$ sans oublier que r et r' sont dans $[\![0, n[\![$.
Que peut-on dire de r et r' ?

Le « si et seulement si » de la propriété signifie que les assertions sont équivalentes, c'est à dire que

- **si** $a \equiv b[n]$, **alors** $a-b$ est un multiple de n
- **ET réciproquement**
- **si** $a-b$ est un multiple de n, **alors** $a \equiv b[n]$

Le « si et seulement si » de la propriété signifie que les assertions sont équivalentes, c'est à dire que

- **si** $a \equiv b[n]$, **alors** $a-b$ est un multiple de n
- **ET réciproquement**
- **si** $a-b$ est un multiple de n, **alors** $a \equiv b[n]$

Le « si et seulement si » de la propriété signifie que les assertions sont équivalentes, c'est à dire que

- **si** $a \equiv b[n]$, **alors** $a - b$ est un multiple de n
- **ET réciproquement**
- **si** $a - b$ est un multiple de n, **alors** $a \equiv b[n]$

Le « si et seulement si » de la propriété signifie que les assertions sont équivalentes, c'est à dire que

- **si** $a \equiv b[n]$, **alors** $a-b$ est un multiple de n
- **ET réciproquement**
- **si** $a-b$ est un multiple de n, **alors** $a \equiv b[n]$


Le « si et seulement si » de la propriété signifie que les assertions sont équivalentes, c'est à dire que

- **si** $a \equiv b[n]$, **alors** $a-b$ est un multiple de n
- **ET réciproquement**
- **si** $a-b$ est un multiple de n, **alors** $a \equiv b[n]$

Cette fois-ci, nous supposons que $a-b$ est un multiple de n, donc il existe un entier k tel que $a-b=kn$.
Or $a-b=n(q-q')+r-r'$, donc $r-r'=n(k-q+q')$.
Que peut-on en déduire sur la différence des restes : $r-r'$?

Cette fois-ci, nous supposons que $a-b$ est un multiple de n, donc il existe un entier k tel que $a-b=kn$.

Or $a-b=n(q-q')+r-r'$, donc $r-r'=n(k-q+q')$.

Que peut-on en déduire sur la différence des restes : $r-r'$?

Cette fois-ci, nous supposons que $a-b$ est un multiple de n, donc il existe un entier k tel que $a-b=kn$.
Or $a-b=n(q-q')+r-r'$, donc $r-r'=n(k-q+q')$.
Que peut-on en déduire sur la différence des restes : $r-r'$?

Cette fois-ci, nous supposons que $a-b$ est un multiple de n, donc il existe un entier k tel que $a-b=kn$.
Or $a-b=n(q-q')+r-r'$, donc $r-r'=n(k-q+q')$.
Que peut-on en déduire sur la différence des restes : $r-r'$?

Conséquence

Cette propriété nous permet en fait d'exploiter autrement les congruences.
En effet, si par exemple $x \equiv 5[32]$, cela signifie qu'il existe un entier k tel que $x-5=32k$, soit encore que $x=5+32k$.

Propriété

$$a \equiv b[n] \Longleftrightarrow \text{il existe un entier } k \text{ tel que } a=b+kn$$

Conséquence

Cette propriété nous permet en fait d'exploiter autrement les congruences.

En effet, si par exemple $x \equiv 5[32]$, cela signifie qu'il existe un entier k tel que $x - 5 = 32k$, soit encore que $x = 5 + 32k$.

Propriété

$$a \equiv b[n] \iff \text{il existe un entier } k \text{ tel que } a = b + kn$$

Conséquence

Cette propriété nous permet en fait d'exploiter autrement les congruences.
En effet, si par exemple $x \equiv 5[32]$, cela signifie qu'il existe un entier k tel que $x - 5 = 32k$, soit encore que $x = 5 + 32k$.

Propriété

$a \equiv b[n] \iff$ *il existe un entier* k *tel que* $a = b + kn$

Conséquence

Cette propriété nous permet en fait d'exploiter autrement les congruences.
En effet, si par exemple $x \equiv 5[32]$, cela signifie qu'il existe un entier k tel que $x - 5 = 32k$, soit encore que $x = 5 + 32k$.

Propriété

$$a \equiv b[n] \iff \textit{il existe un entier } k \textit{ tel que } a = b + kn$$

Ça ressemble à la division euclidienne de a par n.
Mais ça peut ne pas l'être : n'oubliez pas que le reste doit obligatoirement être positif et strictement inférieur au diviseur.
Par exemple on a bien $33 \equiv 97[32]$, mais 97 n'est certes pas le reste de la division de 33 par 32.

Ça ressemble à la division euclidienne de a par n.

Mais ça peut ne pas l'être : n'oubliez pas que le reste doit obligatoirement être positif et strictement inférieur au diviseur. Par exemple on a bien $33 \equiv 97[32]$, mais 97 n'est certes pas le reste de la division de 33 par 32.

Ça ressemble à la division euclidienne de a par n.
Mais ça peut ne pas l'être : n'oubliez pas que le reste doit obligatoirement être positif et strictement inférieur au diviseur.
Par exemple on a bien $33 \equiv 97[32]$, mais 97 n'est certes pas le reste de la division de 33 par 32.

Ça ressemble à la division euclidienne de a par n.
Mais ça peut ne pas l'être : n'oubliez pas que le reste doit obligatoirement être positif et strictement inférieur au diviseur.
Par exemple on a bien $33 \equiv 97[32]$, mais 97 n'est certes pas le reste de la division de 33 par 32.

Propriétés calculatoires

Propriétés

- $a \equiv a[n]$
- *Si* $a \equiv b[n]$, *alors* $b \equiv a[n]$
- *Si* $a \equiv b[n]$ *et* $b \equiv c[n]$, *alors* $a \equiv c[n]$
- *Si* $a \equiv b[n]$ *et* $a' \equiv b'[n]$, *alors*

$$a + a' \equiv b + b' \ [n] \quad a - a' \equiv b - b' \ [n] \quad aa' \equiv bb' \ [n]$$

- *Si* $a \equiv b[n]$, *alors, pour tout* $p \in \mathbb{N}$, $a^p \equiv b^p[n]$

Propriétés calculatoires

Propriétés

- $a \equiv a[n]$
- *Si* $a \equiv b[n]$, *alors* $b \equiv a[n]$
- *Si* $a \equiv b[n]$ *et* $b \equiv c[n]$, *alors* $a \equiv c[n]$
- *Si* $a \equiv b[n]$ *et* $a' \equiv b'[n]$, *alors*

$$a + a' \equiv b + b' \ [n] \quad a - a' \equiv b - b' \ [n] \quad aa' \equiv bb' \ [n]$$

- *Si* $a \equiv b[n]$, *alors, pour tout* $p \in \mathbb{N}$, $a^p \equiv b^p[n]$

Propriétés calculatoires

Propriétés

- $a \equiv a[n]$
- *Si* $a \equiv b[n]$, *alors* $b \equiv a[n]$
- *Si* $a \equiv b[n]$ *et* $b \equiv c[n]$, *alors* $a \equiv c[n]$
- *Si* $a \equiv b[n]$ *et* $a' \equiv b'[n]$, *alors*

$$a + a' \equiv b + b' \ [n] \quad a - a' \equiv b - b' \ [n] \quad aa' \equiv bb' \ [n]$$

- *Si* $a \equiv b[n]$, *alors, pour tout* $p \in \mathbb{N}$, $a^p \equiv b^p[n]$

Propriétés calculatoires

Propriétés

- $a \equiv a[n]$
- *Si* $a \equiv b[n]$, *alors* $b \equiv a[n]$
- *Si* $a \equiv b[n]$ *et* $b \equiv c[n]$, *alors* $a \equiv c[n]$
- *Si* $a \equiv b[n]$ *et* $a' \equiv b'[n]$, *alors*

$$a + a' \equiv b + b' \ [n] \quad a - a' \equiv b - b' \ [n] \quad aa' \equiv bb' \ [n]$$

- *Si* $a \equiv b[n]$, *alors, pour tout* $p \in \mathbb{N}$, $a^p \equiv b^p[n]$

Propriétés calculatoires

Propriétés

- $a \equiv a[n]$
- *Si* $a \equiv b[n]$, *alors* $b \equiv a[n]$
- *Si* $a \equiv b[n]$ *et* $b \equiv c[n]$, *alors* $a \equiv c[n]$
- *Si* $a \equiv b[n]$ *et* $a' \equiv b'[n]$, *alors*

$$a + a' \equiv b + b' \ [n] \quad a - a' \equiv b - b' \ [n] \quad aa' \equiv bb' \ [n]$$

- *Si* $a \equiv b[n]$, *alors, pour tout* $p \in \mathbb{N}$, $a^p \equiv b^p[n]$

Propriétés calculatoires

Propriétés

- $a \equiv a[n]$
- *Si* $a \equiv b[n]$, *alors* $b \equiv a[n]$
- *Si* $a \equiv b[n]$ *et* $b \equiv c[n]$, *alors* $a \equiv c[n]$
- *Si* $a \equiv b[n]$ *et* $a' \equiv b'[n]$, *alors*

$$a + a' \equiv b + b' \ [n] \quad a - a' \equiv b - b' \ [n] \quad aa' \equiv bb' \ [n]$$

- *Si* $a \equiv b[n]$, *alors, pour tout* $p \in \mathbb{N}$, $a^p \equiv b^p[n]$