Chapitre 1
Divisibilité et congruence

$\mathbb{Z}$ désigne l'ensemble des **entiers relatifs** et $\mathbb{N}$ l'ensemble des **entiers naturels**.

I. Divisibilité dans $\mathbb{Z}$

1) Définition

Définition :
On considère deux entiers relatifs a et b, avec $b \neq 0$.
On dit que ***b* divise *a*** et note $b \mid a$ s'il existe un entier relatif k tel que $a = k \times b$.
On dit que ***b* est un diviseur de *a*** et que ***a* est un multiple de *b***.

Exemples :
- $32 = (-4) \times (-8)$; $-8 \in \mathbb{Z}$ donc -4 est un diviseur de 32.
- L'ensemble des multiples de 3 est {… ; -6 ; -3 ; 0 ; 3 ; 6 ; …}. On le note $3\mathbb{Z}$.
- Soit $n \in \mathbb{Z}$, on a $n^2 - 1 = (n-1)(n+1)$; $n-1 \in \mathbb{Z}$ donc si $n \neq -1$, alors $n+1$ est un diviseur de $n^2 - 1$.

Remarques :
- $a = k \times b$ peut aussi s'écrire $a = (-k) \times (-b)$, donc si b divise a, alors $(-b)$ aussi divise a.
  $a = k \times b$ peut aussi s'écrire $-a = (-k) \times b$, donc si b divise a, alors b aussi divise $-a$.
  Ainsi la recherche des diviseurs d'un entier relatif a dans $\mathbb{Z}$ se ramène à la recherche des diviseurs de l'entier naturel $|a|$ dans $\mathbb{N}$.
- Tous les entiers relatifs non nuls sont des diviseurs de 0 (0 est multiple de tous les entiers).
- Tout entier n non nul a pour diviseurs : 1, -1, n et $-n$.
  Il a un nombre fini de diviseurs tous compris entre $-n$ et n.
- Un entier non nul a une infinité de multiples.

Définition :
Deux entiers relatifs sont **premiers entre eux** si leurs seuls diviseurs communs sont -1 et 1.

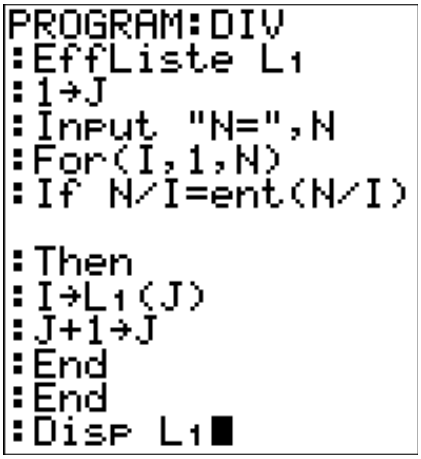
Exemple :
Les diviseurs de 18 sont 1, 2, 3, 6, 9, 18 et leurs opposés. Ceux de 12 sont 1, 2, 3, 4, 6, 12 et leurs opposés.
Les diviseurs communs à 12 et 18 sont donc 1, 2, 3, 6 et leurs opposés.
Donc 12 et 18 ne sont pas premiers entre eux.

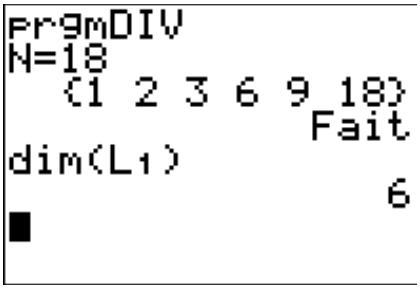
Algorithme :

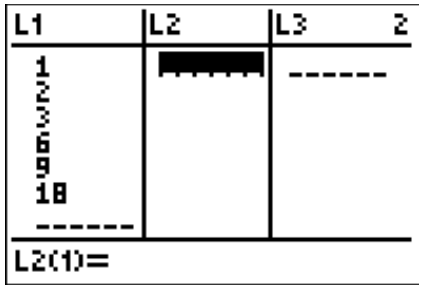
Ent(x) représente la fonction partie entière de x.

Entrée
Lire N
Traitement :
Pour i allant de 1 jusqu'à N
Si N/i=Ent(N/i) Alors
Afficher i
Fin Si
Fin Pour

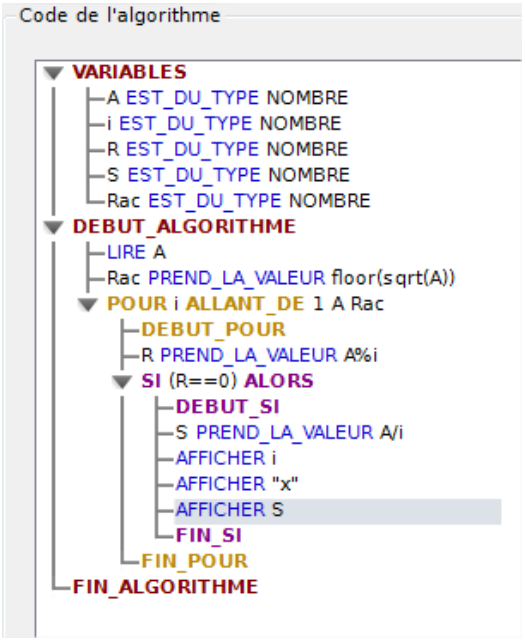
Calculatrice

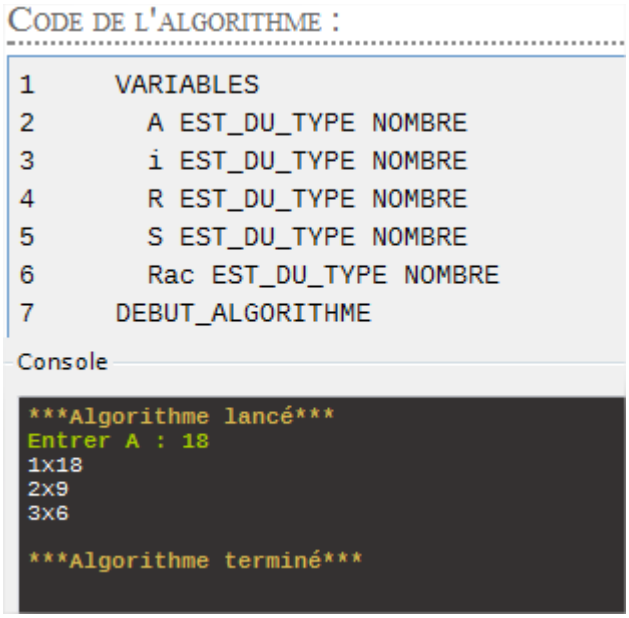




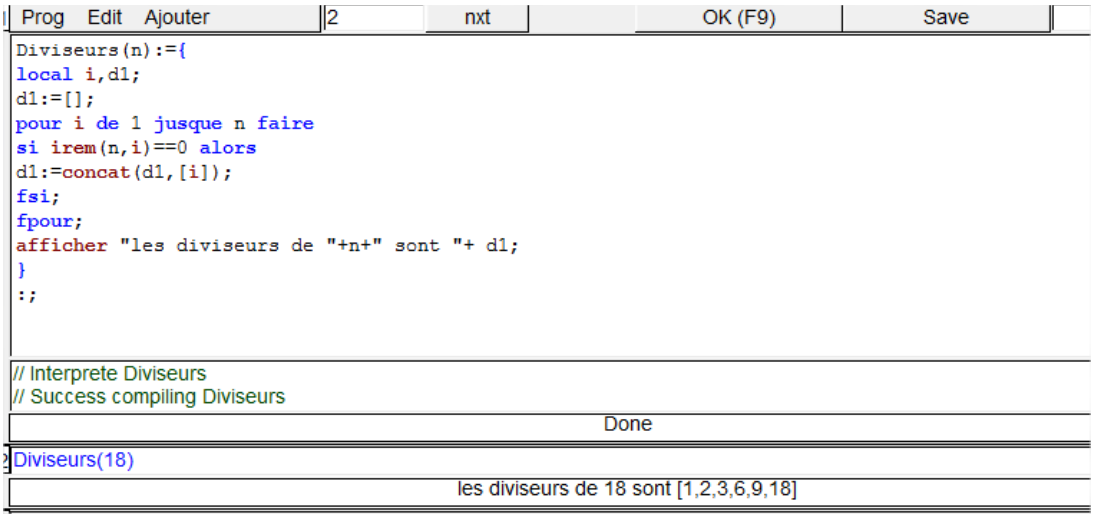


Algobox





Xcas



2) *Propriétés*

Propriété (transitivité) :
Soit a, b, c trois entiers relatifs non nuls.
Si c divise b et b divise a alors c divise a.

Démonstration :
Comme c divise b et b divise a, il existe des entiers k et k' tels que $b=kc$ et $a=k'b$, d'où $a=(k'k)c$ et $k'k\in\mathbb{Z}$. Donc c divise a.

Exemple :
4 divise 8 et 8 divise 80 donc 4 divise 80.

Remarque :
Si a divise b et si b divise a alors a et b sont égaux ou opposés.

Propriété (combinaison linéaire) :
Soit a, b, c trois entiers relatifs non nuls.
Si c divise a et b alors, pour tous entiers relatifs u et v, c divise $ua+vb$.

Démonstration :
Comme c divise a et c divise b, il existe des entiers k et k' tels que $a=kc$ et $b=k'c$, alors pour tous entiers relatifs u et v :
$ua+vb=ukc+vk'c=(uk+vk')c$ avec $(uk+vk')\in\mathbb{Z}$, d'où c divise $ua+vb$.

Remarque :
Si a divise b et si a divise c alors a divise $b+c$ et $b-c$.

Exemples :

- Soit a et n deux entiers naturels ; si a divise $3n+12$ et si a divise $n+3$ alors a divise $3n+12-3(n+3)$. Donc a divise 3 et donc les valeurs possibles de a sont {-3 ; -1 ; 1 ; 3}
- Soit n un entier. Si c divise n et $n+1$ alors c divise $n+1-n=1$ donc $c=1$ ou $c=-1$. Ainsi les entiers n et $n+1$ sont premiers entre eux.

II. Division euclidienne

1) Division euclidienne dans $\mathbb{N}$

Théorème :
Pour tout entier naturel *a* et pour tout entier naturel *b* non nul, il **existe** un **unique** couple $(q;r)$ d'entiers naturels tels que :

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

q est le **quotient** et *r* le **reste** de la **division euclidienne** de *a* par *b*.

Démonstration :

Propriété d'Archimède :
Pour tout entier naturel a et tout entier naturel b non nul, il existe un entier naturel n tel que $a<nb$ *. (il suffit de prendre* $n=a+1$ *).*
On dit que $\mathbb{N}$ *est archimédien (en faisant suffisamment de « pas » de longueur* $b\neq 0$*, on peut toujours dépasser a).*
Propriété (admise) :
Une partie de $\mathbb{N}$ *non vide admet un plus petit élément. (Cette propriété est fausse dans* $\mathbb{Z}$ *ou dans* $\mathbb{R}$*).*

On considère un entier a et un entier non nul b.

- ***Existence du couple*** $(q;r)$

D'après la propriété d'Archimède, l'ensemble A des entiers naturels n tels $a<nb$ *n'est pas vide ; donc il admet un plus petit élément* m_0 *.*
Si $m_0=0$*, alors* $a<0$ *: c'est impossible car a est un entier naturel.*
Comme m_0 *est le plus petit élément de A, on a* $(m_0-1)b\leqslant a$ *.*
On pose $q=m_0-1$*, on obtient* $qb\leqslant a<(q+1)b$ *.*
En retranchant qb *à chaque expression, on aboutit à* $0\leqslant a-qb<b$ *.*
En posant $r=a-bq$*, on obtient bien* $a=bq+r$ *et* $0\leqslant r<b$ *.*
D'où l'existence du couple $(q;r)$ *.*

- ***Unicité du couple*** $(q;r)$

On suppose que $a=bq_1+r_1=bq_2+r_2$ *où* $0\leqslant r_1<b$ *et* $0\leqslant r_2<b$ *.*
On a donc $-b<r_1-r_2<b$ *et* $r_1-r_2=b(q_1-q_2)$*, ce qui signifie que* r_1-r_2 *est un multiple de b strictement compris entre* $-b$ *et b. Ainsi* $r_1-r_2=0$ *d'où* $r_1=r_2$ *.*
Comme $b\neq 0$*, on obtient* $q_1=q_2$ *. Le couple* $(q;r)$ *est unique.*

Exemple :
Division euclidienne de 43 par 5 :
On a $43=5\times 8+3$.
Le quotient est 8 et le reste est 3.

4	3	5
	3	8

Remarque :
Si *a* et *b* sont deux entiers naturels quelconques avec *b* non nul, alors on a :
a est divisible par *b* si, et seulement si, le reste de la division euclidienne de *a* par *b* est nul.

Exemple :
Aurélien possède n CD. S'il les empile par 10 il lui en reste 7 et s'il les empile par 7 il a 22 piles de plus et il lui en reste 3.

- « S'il les empile par 10 il lui en reste 7 » se traduit par : il existe $q \in \mathbb{N}$ tel que $n = 10q+7$.
- « S'il les empile par 7 il lui en reste 3 » se traduit par : il existe $q' \in \mathbb{N}$ tel que $n = 7q'+3$.
- « Il a 22 piles de plus » se traduit par $q' = q+22$.

D'où $\begin{cases} n = 10q+7 \\ n = 7(q+22)+3 \end{cases} \Leftrightarrow \begin{cases} n = 10q+7 \\ 10q+7 = 7(q+22)+3 \end{cases} \Leftrightarrow \begin{cases} n = 10q+7 \\ 3q = 150 \end{cases}$

Soit $\begin{cases} q = 50 \\ n = 10\times 50+7 = 507 \end{cases}$.

Aurélien possède 507 CD.
Pour que ses piles comportent le même nombre de CD, il faut que le nombre de CD par pile divise 507. Il peut donc faire des piles de 3, 13, 39 ou 169 CD.

Propriété :
Dans la division euclidienne de a par b, il y a b restes possibles : 0, 1, … , $b-1$.

Exemple :
Tout entier a pour reste 0, 1, 2 ou 3 dans la division par 4 donc s'écrit sous la forme $4k$, $4k+1$, $4k+2$ ou $4k+3$ avec k entier.

Interprétation graphique :
On encadre a par deux entiers consécutifs de b.

2) *Division euclidienne dans $\mathbb{Z}$*

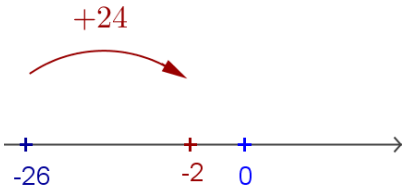
Théorème :
Pour tout entier relatif a et pour tout entier relatif b non nul, il existe un unique couple $(q;r)$ d'entiers relatifs tels que :

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

q est le **quotient** et r le **reste** de la **division euclidienne** de a par b.

Exemples :

- $-2 = 26\times(-1)+24$ est la relation de la division euclidienne de -2 par 26 avec pour quotient -1 et pour reste 24.



- $a = 2013$ et $b = 7$: $2013 = 7\times 287+4$ et $0 \leqslant 4 < 7$. Donc $q = 287$ et $r = 4$.
- $a = 2013$ et $b = -7$: $2013 = (-7)\times(-287)+4$ et $0 \leqslant 4 < |-7|$. Donc $q = -287$ et $r = 4$.
- $a = -2013$ et $b = 7$: $-2013 = 7\times(-287)-4 = 7\times(-288)+3$ et $0 \leqslant 3 < 7$. Donc $q = -288$ et $r = 3$.
- $a = -2013$ et $b = -7$: $-2013 = (-7)\times 288+3$ Et $0 \leqslant 3 < |-7|$. Donc $q = 288$ et $r = 3$.

Algorithme : division euclidienne dans $\mathbb{N}$

Entrée

Lire a

Lire b

Traitement :

q prend la valeur 0

Tant que $a \geqslant b \times q$ faire

q prend la valeur $q+1$

Fin Tant que

q prend la valeur $q-1$

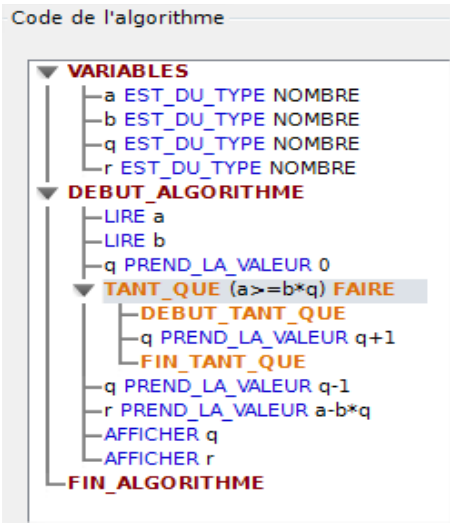
r prend la valeur $a-b \times q$

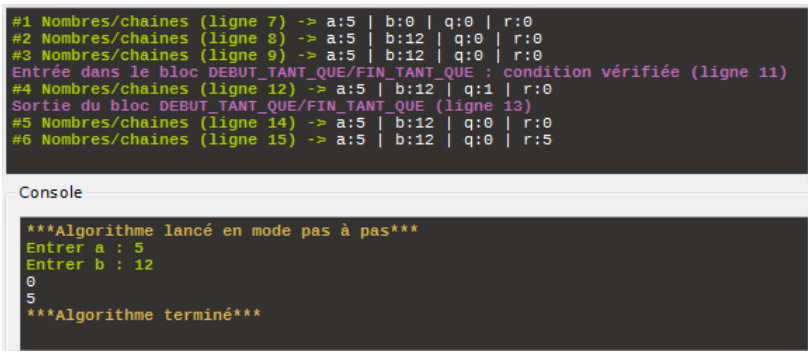
Sortie

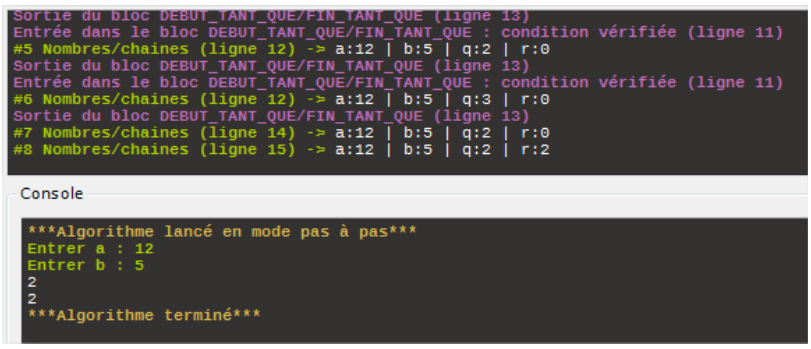
Afficher q

Afficher r

Algobox







Calculatrice (dans $\mathbb{N}$ puis dans $\mathbb{Z}$)

```
PROGRAM:BASEDIV
:0→Q
:While A≥B*Q
:Q+1→Q
:End
:Q-1→Q
:A-B*Q→R
```

```
PROGRAM:DIVN
:Input "A=",A
:Input "B=",B
:prgmBASEDIV
:Disp "Q=",Q
:Disp "R=",R
```

```
PROGRAM:DIVZ
:Input "A=",A
:Input "B=",B
:If A≥0 et B>0
:Then
:prgmBASEDIV
:End
:If A≥0 et B<0
:Then
: -B→B
:prgmBASEDIV
: -Q→Q
:End
:If A<0 et B>0
:Then
: -A→A
:prgmBASEDIV
:If R=0
:Then
: -Q→Q
:Else
: -(Q+1)→Q
:B-R→R
:End
:End
:If A<0 et B<0
:Then
: -A→A
: -B→B
:prgmBASEDIV
:If R≠0
:Then
:Q+1→Q
:B-R→R
:End
:End
:Disp "Q=",Q
:Disp "R=",R
```

```
prgmDIVN
A=2013
B=7
```

```
A=2013
B=7
Q=
                287
R=
                  4
              Fait
```

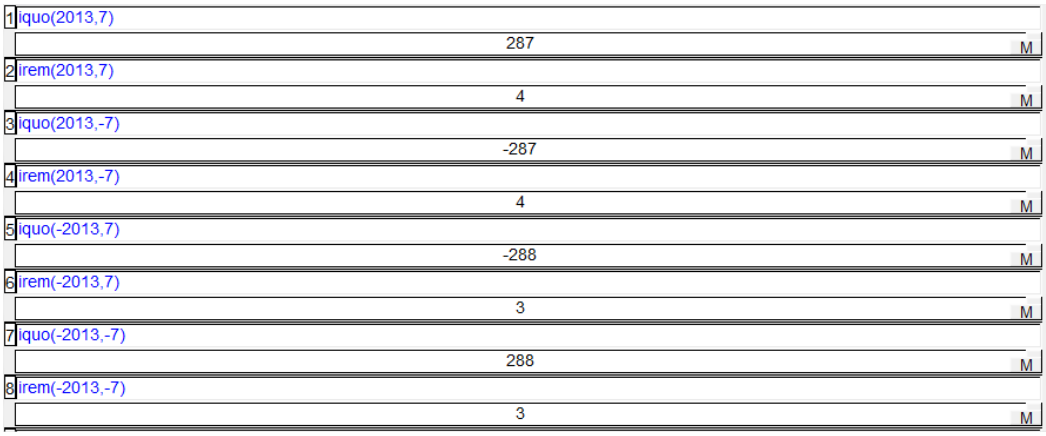
```
prgmDIVZ
A=2013
B=-7
```

```
A=2013
B=-7
Q=
               -287
R=
                  4
              Fait
```

```
A=-2013
B=7
Q=
               -288
R=
                  3
              Fait
```

```
A=-2013
B=-7
Q=
                288
R=
                  3
              Fait
```

Xcas



III. Congruences dans $\mathbb{Z}$

1) Définition

Définition :
Soit n un entier naturel non nul, a et b deux entiers relatifs quelconques.
On dit que ***a* est congru à *b* modulo *n***, et on note $a \equiv b\,[n]$ si a et b ont **même reste** dans la division euclidienne par n.

Remarques :
- On dit aussi que a et b sont congrus modulo n.
- On le note également $a \equiv b\,(n)$ ou $a \equiv b \mod n$ ou $a \equiv b$ modulo n.

Conséquence :
$a \equiv r\,[n]$ avec $0 \leqslant r < n$ $\Leftrightarrow$ a a pour reste r dans la division euclidienne par n.

Exemple :
$145 = 13 \times 11 + 2$ et $119 = 13 \times 9 + 2$ donc $145 \equiv 119\,[13]$.

Propriété :
Soit n un entier naturel non nul, a et b deux entiers relatifs quelconques.
$a \equiv b\,[n]$ si, et seulement si, n divise $a - b$.

Démonstration :
On effectue la division euclidienne de a par n puis de b par n, il existe alors un couple d'entiers relatifs $(q\,;q')$ et un couple d'entiers naturels $(r\,;r')$ tels que :
$a = qn + r$ avec $0 \leqslant r < n$ et $b = q'n + r'$ avec $0 \leqslant r' < n$.

- Sens direct : on suppose $a \equiv b\,[n]$

Alors par définition, a et b ont le même reste dans la division euclidienne par n.
Ainsi $r = r'$ d'où $a = qn + r$ et $b = q'n + r$ avec $0 \leqslant r < n$.
Par suite, $a - b = n(q - q')$ avec $q - q' \in \mathbb{Z}$. Donc n divise $a - b$.

- Sens réciproque : on suppose que n divise $a - b$.

Alors il existe $k \in \mathbb{Z}$ tel que $a - b = kn$.
Or $a - b = (qn + r) - (q'n + r') = n(q - q') + (r - r')$, donc :
$n(q - q') + (r - r') = kn$, par suite $r - r' = n(k - q + q')$.
Or $0 \leqslant r < n$ et $0 \leqslant r' < n$ donc $-n < r - r' < n$.
Soit $-n < n(k - q + q') < n$ d'où $-1 < k - q + q' < 1$ car $n > 0$.
Ainsi $k - q + q' = 0$ et, par suite $r - r' = 0$, soit $r = r'$.
Donc a et b ont le même reste dans la division euclidienne par n.

Exemple :
$145 - 119 = 26 = 2 \times 13$ donc $145 \equiv 119\,[13]$.

Conséquences :
- $a \equiv 0\,[n]$ $\Leftrightarrow$ a est divisible par n.
- Transitivité :
  Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$ alors $a \equiv c\,[n]$.
- Les nombres congrus à b modulo c sont les nombres $b + kc$, $k \in \mathbb{Z}$.

Exemple :
À quel jour de la semaine correspond le 25 juillet 1137 ? (le 1er janvier 2012 était un dimanche)
Il y a 874 années complètes.
$874=4\times218+2$ donc il y a 218 années bissextiles et 656 années complètes.
Du 25 juillet 1137 au 31 décembre 1137 se sont écoulés 160 jours ($7+31\times3+30\times2$)
Entre le 25 juillet 1137 et le 1er janvier 2012 se sont écoulés :
$160+218\times366+656\times365+1=319389$
Or $319389\equiv0[7]$ donc le 25 juillet 1137 était un dimanche.

2) Opérations

Propriétés :
Soit n un entier naturel non nul, a, b, c et d quatre entiers relatifs.
Si $a\equiv b[n]$ et $c\equiv d[n]$ alors :

$$a+c\equiv b+d[n] \quad \text{et} \quad ac\equiv bd[n]$$

Démonstrations :
Par hypothèse, il existe k et k' entiers tels que : $a=b+kn$ et $c=d+k'n$.

- Donc $a+c=b+d+(k+k')n$ avec $k+k'\in\mathbb{Z}$.
  Par suite $a+c\equiv b+d[n]$.
- $ac=(b+kn)(d+k'n)=bd+n(bk'+kd+nkk')$ avec $bk'+kd+nkk'\in\mathbb{Z}$.
  Par suite $ac\equiv bd[n]$

Exemple :
$59\equiv3[7]$ et $48\equiv6[7]$.
On en déduit que $59+48\equiv3+6[7]$, soit $59+48\equiv9[7]$ et donc $107\equiv2[7]$.
De même $59\times48\equiv3\times6[7]$ d'où $2832\equiv18[7]\equiv4[7]$.

Conséquences :
Soit n un entier naturel non nul, a, b et k des entiers relatifs.
Si $a\equiv b[n]$ alors :

- $a+k\equiv b+k[n]$
- $ka\equiv kb[n]$
- Pour tout $p\in\mathbb{N}$, $a^p\equiv b^p[n]$.

Remarque :
La réciproque de chacune des propriétés :
« Si $a\equiv b[n]$ alors $ka\equiv kb[n]$ » et « si $a\equiv b[n]$ alors, pour tout $p\in\mathbb{N}$, $a^p\equiv b^p[n]$ »
est fausse :

- $22\equiv18[4]$ mais 11 et 9 ne sont pas congrus modulo 4.
- $5^2\equiv2^2[7]$ mais 5 et 2 ne sont pas congrus modulo 7.

Exemple :
Mathias, Aline, Tatiana et Hélène forment des paquets de 10 cartes, m, a, t et h désignent respectivement leur nombre de cartes. Il reste 2 cartes à Mathias et 4 cartes à Aline. Il reste à Tatiana deux fois plus de cartes qu'à Aline et il reste à Hélène cinq cartes de plus qu'à Mathias.
S'ils regroupent tous leurs cartes et forment des piles de 10 cartes, combien de cartes restent-ils ?
$m\equiv2[10]$ et $a\equiv4[10]$ et $t\equiv2a[10]$ et $h\equiv m+5[10]$
Donc, $t\equiv8[10]$ et $h\equiv7[10]$. Par suite $m+a+t+h\equiv21[10]\equiv1[10]$. Il reste donc une carte.