Congruences. Critères de divisibilité.

1. Congruences

1.1. Division euclidienne dans $\mathbb{Z}$

Soit a un <u>entier relatif</u> et b un <u>entier naturel non nul</u> alors il existe un unique couple $(q;r)$, q entier relatif et r entier naturel vérifiant:

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

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

1.2. Activité

a)

✔ Quels sont les restes de la division euclidienne par 5 des nombres -27; -12; 37 et 52

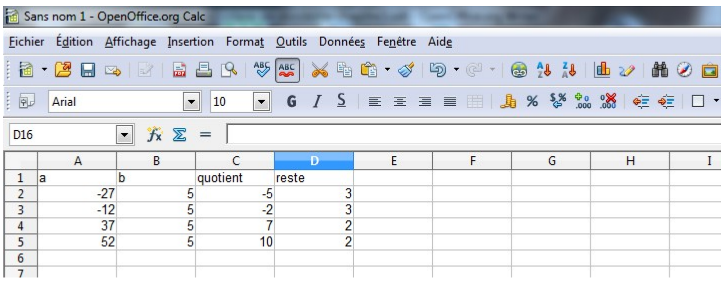
$-27=5\times(-6)+3$	$q=-6$	$r=3$
$-12=5\times(-3)+3$	$q=-3$	$r=3$
$37=5\times7+2$	$q=7$	$r=2$
$52=5\times10+2$	$q=10$	$r=2$

On peut aussi utiliser le tableur:

On tape:

En A1:a	En B1:b	En C1: quotient	En D1: reste
En A2: -27	En B2: 5	En C2: « =quotient (A2;B2) »	En D2: « =mod(A2;B2)
En A3: -12	En B3: 5	En C3 et D3, on étire les formule de C2 et D2	

Etc...



	A	B	C	D
1	a	b	quotient	reste
2	-27	5	-5	3
3	-12	5	-2	3
4	37	5	7	2
5	52	5	10	2

✔ Soit a un entier relatif dont le reste de la division euclidienne par 5 est 2. Que devient ce reste si on ajoute à a un multiple de 5?

$a=5q+2$ avec $q\in\mathbb{Z}$

Soit $b=5k$ avec $k\in\mathbb{Z}$ est un multiple de 5

$a+b=5q+2+5k=5(q+k)+2$ avec $q+k\in\mathbb{Z}$

Donc le reste de la division euclidienne de b par 5 est aussi 2.

✔ a et a' sont deux entiers relatifs admettant 2 comme reste dans la division euclidienne par 5. Que peut-on dire de $a-a'$?

$a=5q+2$ avec $q\in\mathbb{Z}$

$a'=5q'+2$ avec $q'\in\mathbb{Z}$

$a-a'=5(q-q')$ avec $q-q'\in\mathbb{Z}$

Donc $a-a'$ est un multiple de 5 dans $\mathbb{Z}$

b) $a=-18$; $a'=12$; $b=29$; $b'=-6$

✔ Quels sont les restes des divisions euclidiennes par 5 de $a;a';b;b'$

$a=5\times(-4)+2$ $q=-4$ $r=2$

$a'=5\times2+2$ $q=2$ $r=2$

$b=5\times5+4$ $q=5$ $r=4$

$b'=5\times(-2)+4$ $q=-2$ $r=4$

✔ Quels sont les restes de la division euclidienne de $a+b$ et de $a'+b'$ par 5?

$a+b=-18+29=11=5\times2+1$ $q=2$ $r=1$

$a'+b'=12-6=6=5\times1+1$ $q=1$ $r=1$

✔ Quels sont les restes de la division euclidienne de $7a-3b$ et $7a'-3b'$ par 5?

$7a-3b$

$=7[5\times(-4)+2]-3[5\times5+4]$

$=5\times(-28)+14+5\times(-15)-12$

$=5\times(-43)+2$ $q=-43$ $r=2$

$7a'-3b'$

$=7[5\times2+2]-3[5\times(-2)+4]$

$=5\times14+14+5\times6-12$

$=5\times20+2$ $q=20$ $r=2$

✔ Quels sont les restes de la division euclidienne de ab et $a'b'$ par 5?

ab

$=-18\times29$

$=-522$

$=5\times(-105)+3$ $q=-105$ $r=3$

$a'b'$
$=12\times(-6)$
$=-72$
$=5\times(-15)+3$ $\quad q=-15 \quad r=3$

✔ Quels sont les restes de la division euclidienne de a^3 ; a'^3 ; b^2 et b'^2 par 5?

a^3
$=-5832$
$=5\times(-1167)+3$ $\quad q=-1167 \quad r=3$

a'^3
$=1728$
$=5\times 345+3$ $\quad q=345 \quad r=3$

b^2
$=841$
$=5\times 168+1$ $\quad q=168 \quad r=1$

b'^2
$=36$
$=5\times 7+1$ $\quad q=7 \quad r=1$

1.3. Définition

n est un entier naturel supérieur ou égal à 2.

Deux entiers relatifs a et a' qui ont le même reste dans la division euclidienne par n sont dits **congrus** modulo n.
On note: $\boxed{a\equiv a'(mod\ n)}$ ou $\boxed{a\equiv a'(n)}$

1.4. Conséquence

n est un entier naturel supérieur ou égal à 2. a et a' deux entiers relatifs.

$\boxed{a\equiv a'(mod\ n)\Leftrightarrow(a-a')\text{ est un multiple de } n}$

1.5. Propriétés

n est un entier naturel supérieur ou égal à 2. a, a', a'' entiers relatifs.
Si $a \equiv a' (mod\ n)$ et si $a' \equiv a'' (mod\ n)$ alors $\boxed{a \equiv a'' (mod\ n)}$

Démonstration:

$a - a'' = (a - a') + (a' - a'')$

$(a - a')$ est un multiple de n ; $(a' - a'')$ est un multiple de n.

Or la somme de deux multiples de n est un multiple de n donc $a - a''$ est un multiple de n et donc:

$a \equiv a'' (mod\ n)$

n est un entier naturel supérieur ou égal à 2. a, a', k entiers relatifs
Si $a \equiv a' (mod\ n)$ alors $\boxed{ka \equiv ka' (mod\ n)}$

Démonstration:

$ka - ka' = k(a - a')$

$(a - a')$ est un multiple de n.

Or tout multiple d'un multiple de n est un multiple de n donc $k(a - a')$ est un multiple de n et donc:

$ka \equiv ka' (mod\ n)$

n est un entier naturel supérieur ou égal à 2. a, a', b, b' entiers relatifs
Si $a \equiv a' (mod\ n)$ et si $b \equiv b' (mod\ n)$ alors $\boxed{a + b \equiv a' + b' (mod\ n)}$

Démonstration:

$(a + b) - (a' + b') = (a - a') + (b - b')$

$(a - a')$ est un multiple de n ; $(b - b')$ est un multiple de n.

Or la somme de deux multiples de n est un multiple de n donc $(a + b) - (a' + b')$ est un multiple de n et donc:

$a + b \equiv a' + b' (mod\ n)$

n est un entier naturel supérieur ou égal à 2. a, a', b, b' entiers relatifs
Si $a \equiv a' (mod\ n)$ et si $b \equiv b' (mod\ n)$ alors $\boxed{ab \equiv a'b' (mod\ n)}$

Démonstration:

$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + b'(a - a')$

$(a - a')$ est un multiple de n ; $(b - b')$ est un multiple de n.

Donc $a(b - b') + b'(a - a')$ est un multiple de n et donc:

$ab \equiv a'b' (mod\ n)$

n est un entier naturel supérieur ou égal à 2. a, a', b, b', k, k' entiers relatifs
Si $a \equiv a' (mod\ n)$ et si $b \equiv b' (mod\ n)$ alors $\boxed{ka + kb \equiv ka' + kb' (mod\ n)}$

Démonstration:
$(ka+kb)-(ka'+kb') = k(a-a')+k(b-b')$
$(a-a')$ est un multiple de n et $(b-b')$ est un multiple de n.
Donc $k(a-a')+k(b-b')$ est un multiple de n et donc:
$ka + kb \equiv ka' + kb' (mod\ n)$

n est un entier naturel supérieur ou égal à 2. a, a' entiers relatifs et p entier naturel non nul
Si $a \equiv a' (mod\ n)$ alors $\boxed{a^p \equiv a'^p (mod\ n)}$

Démonstration:
On peut effectuer un raisonnement par récurrence sur p.
ou:
$a^p - a'^p = (a-a')(a^{p-1} + a^{p-2} a' + a^{p-3} a'^2 + ... + aa'^{p-2} + a'^{p-1})$
(a-a') est un multiple de n donc $(a-a')(a^{p-1}+a^{p-2}a'+a^{p-3}a'^2+ \ldots +aa'^{p-2}+a'^{p-1})$ est un multiple de n et donc:
$a^p \equiv a'^p (mod\ n)$

n est un entier naturel supérieur ou égal à 2. a entier relatif et d entier naturel non nul
Si $a \equiv d (mod\ n)$ avec $0 \leqslant d < n$ alors d est **le reste de la division euclidienne** de a par n.

Démonstration:
$a \equiv d (mod\ n)$ donc $a-d$ est un multiple de n, donc il existe tel $k \in \mathbb{Z}$ que:
$a-d = nk$
$a = nk + d$

On effectue la division euclidienne de a par n:
$a = nq + r \qquad q \in \mathbb{Z}$ et $0 \leqslant r < n$
Par unicité du couple (q; r) de la division euclidienne $r = d$

Remarque importante:

n est un entier naturel supérieur ou égal à 2. a, b, k entiers relatifs
Si $ka \equiv kb (mod\ n)$, on n'a pas nécessairement $a \equiv b (mod\ n)$

Démonstration:

$n=4 \quad a=8 \quad b=10 \quad k=2$

$ka=16 \qquad ka\equiv 0(4)$

$kb=20 \qquad kb\equiv 0(4)$

Donc $ka\equiv kb(4)$

$a\equiv 0(4)$ et $b\equiv 2(4)$

a et b n'ont pas le même reste dans la division euclidienne par 4 donc a et b ne sont pas congrus modulo 4.

1.6. Exercices

a) Déterminer les restes de la division euclidienne de 2^p $p\in\mathbb{N}$ par5.

$2^0=1\equiv 1(5)$ Le reste de la division euclidienne de 2^0 par 5 est 1.

$2^1=2\equiv 2(5)$ Le reste de la division euclidienne de 2^1 par 5 est 2.

$2^2=4\equiv 4(5)$ Le reste de la division euclidienne de 2^2 par 5 est 4.

$2^3=8\equiv 3(5)$ Le reste de la division euclidienne de 2^3 par 5 est 3.

$2^4=16\equiv 1(5)$ Le reste de la division euclidienne de 2^4 par 5 est 1.

Tout entier naturel p peut s'écrire $p=4k$ ou $p=4k+1$ ou $p=4k+2$ ou $p=4k+3$ avec $k\in\mathbb{N}$ car le reste de la division euclidienne de p par 4 est soit égal à 0; 1; 2 ou 3.

Si $p=4k$

$2^p=2^{4k}=(2^4)^k$

Or, $2^4\equiv 1(5)$

Donc $(2^4)^k\equiv 1^k(5)$

Par suite, $2^p\equiv 1(5)$

Le reste de la division euclidienne de 2^p par 5 est 1.

Si $p=4k+1$

$2^p=2^{4k+1}=2^{4k}\times 2^1$

Or, $2^{4k}\equiv 1(5)$

Donc $2^{4k}\times 2^1\equiv 1\times 2(5)$

Par suite, $2^{4k+1}\equiv 2(5)$

Le reste de la division euclidienne de 2^p par 5 est 2.

Si $p=4k+2$

$2^p=2^{4k+2}=2^{4k}\times 2^2$

Or, $2^{4k}\equiv 1(5)$

Donc $2^{4k}\times 2^2\equiv 1\times 2^2(5)$

Par suite, $2^{4k+2} \equiv 4(5)$

Le reste de la division euclidienne de 2^p par 5 est 4.

Si $p=4k+3$

$2^p=2^{4k+3}=2^{4k}\times 2^3$

Or, $2^{4k}\equiv 1(5)$

Donc $2^{4k}\times 2^3\equiv 1\times 2^3(5)$

Par suite, $2^{4k+3}\equiv 8(5)$

Par suite, $2^{4k+3}\equiv 3(5)$

Le reste de la division euclidienne de 2^p par 5 est 3.

<u>Exemple:</u>

Quel est le reste de la division euclidienne de 2^{2011} par 5

$2011=4\times 502+3$

donc $2011=4k+3$ avec $k=502$

Donc $2011\equiv 3(5)$

Le reste de la division euclidienne de 2011 par 5 est 3.

b)

- ✔ Déterminer les restes de la division euclidienne de 3^p par 4 $(p\in\mathbb{N})$
- ✔ Déterminer les restes de la division euclidienne de 3^p par 7 $(p\in\mathbb{N})$
- ✔ En déduire que $3^{1998}-1$ est divisible par 4 et 7.

✔ $3^1=3\equiv 3(4)$

$3^2=9\equiv 1(4)$

Donc, pour $k\in\mathbb{N}$, $3^{2k}\equiv 1(4)$ et $3^{2k+1}\equiv 3(4)$

✔ $3^0=1\equiv 1(7)$

$3^1=3\equiv 3(7)$

$3^2=9\equiv 2(7)$

$3^3=3\times 3^2\equiv 3\times 2(7)$ donc $3^3\equiv 6(7)$

$3^4=3\times 3^3\equiv 3\times 6(7)$ donc $3^4\equiv 18(7)$ donc $3^4\equiv 4(7)$

$3^5=3\times 3^4\equiv 12(7)$ donc $3^5\equiv 5(7)$

$3^6=3\times 3^5\equiv 15(7)$ donc $3^6\equiv 1(7)$

Pour $k \in \mathbb{N}$, les restes des divisions euclidiennes de $3^{6k} ; 3^{6k+1} ; 3^{6k+2} ; 3^{6k+3} ; 3^{6k+4} ; 3^{6k+5}$ sont respectivement 1; 3; 2; 6; 4; 5

✔ $1998 = 2 \times 999$

Donc $3^{1998} \equiv 1(4)$

$3^{1998} - 1 \equiv 0(4)$

Donc $3^{1998} - 1$ est divisible par 4

$1998 = 6 \times 333$

Donc $3^{1998} \equiv 1(7)$

$3^{1998} - 1 \equiv 0(7)$

Donc $3^{1998} - 1$ est divisible par 7

2. Critères de divisibilité dans le système décimal

$a \in \mathbb{N} \quad a = \overline{mcdu}$

$u \in \mathbb{N} \quad 0 \leqslant u \leqslant 9$

$d \in \mathbb{N} \quad 0 \leqslant d \leqslant 9$

$c \in \mathbb{N} \quad 0 \leqslant c \leqslant 9$

$m \in \mathbb{N} \quad 0 \leqslant m \leqslant 9$

$a = 3 \times 10^3 + c \times 10^2 + d \times 10 + u$

2.1. Critère de divisibilité par 2 et 5

$10 = 2 \times 5$

2 et 5 sont des diviseurs de 10

Donc, $10 \equiv 0(2)$ et $10 \equiv 0(5)$

Par suite, pour tout $n \in \mathbb{N}^*$

$10^n \equiv 0(2)$ et $10^n \equiv 0(5)$

Donc, $a \equiv u(2)$ et $a \equiv u(5)$

Un entier naturel a est **divisible par 2** (respectivement **par 5**) si et seulement si **son chiffre des unités en numération décimale est divisible par 2** (respectivement **par 5**)

2.2. Critères de divisibilité par 4 et 25

$4=2^2$; $25=5^2$ et $4\times 25=100=10^2$

Donc, $10^2\equiv 0(4)$ et $10^2\equiv 0(25)$

$10^3=10\times 10^2\equiv 0(4)$ et $10^3=10\times 10^2\equiv 0(25)$

Par suite, pour tout $n\in\mathbb{N}$, $n\geq 2$

$10^n\equiv 0(4)$ et $10^n\equiv 0(25)$

Donc:

$a\equiv d\times 10+u(4)$ et $a\equiv d\times 10+u(25)$

$a\equiv\overline{du}(4)$ et $a\equiv\overline{du}(25)$

Un entier naturel a est **divisible par 4** (respectivement **par 25**) si et seulement si **le nombre formé par ses deux derniers chiffres en numération décimale est divisible par 4** (respectivement **par 25**)

2.3. Critères de divisibilité par 3 et 9

$10\equiv 1(3)$ et $10\equiv 1(9)$
Donc, pour tout $n\in\mathbb{N}$
$10^n\equiv 1(3)$ et $10^n\equiv 1(9)$
Par suite,
$a\equiv m+c+d+u(3)$ et $a\equiv m+c+d+u(9)$

Un entier naturel a est **divisible par 3** (respectivement **par 9**) si et seulement si **la somme de ses chiffres en numération décimale est divisible par 3** (respectivement **par 9**).

2.4. Critères de divisibilité par 11

$10\equiv -1(11)$
Donc, pour tout $n\in\mathbb{N}$
$10^n\equiv(-1)^n(11)$
Par suite,
$a\equiv -m+c-d+u(11)$

Un entier naturel a est congru modulo 11 à la somme des ses chiffres de rangs pairs (en partant du chiffre des unités) diminuée de la somme de ses chiffres de rangs impairs.

Un entier naturel a est **divisible par 11** si et seulement **si la somme des ses chiffres de rangs pairs (en partant du chiffre des unités) diminuée de la somme de ses chiffres de rangs impairs est un multiple de 11.**

Exemple:
$251139\equiv 9+1+5-(3+1+2)(11)$ et donc $251139\equiv 9(11)$