# calculs modulo *n*

par Claire Lapouille (2nde), Sébastien Pontillo (2nde), Magali Stablo ($TA_1$), Stéphanie Vandevoorde (2nde), élèves du lycée Alfred Kastler de Cergy (95)

enseignantes : Claude Matz, Annie Soismier

chercheurs : Daniel Barsky et François Digne

---

lettre de Mmes Annie Soismier et Claude Matz, animatrices “MATh.en.JEANS” au lycée Alfred Kastler pendant l’année 1994-95, postée de Cergy, le 15 octobre 1994.

« Nous nous sommes décidées, après de longues hésitations, à publier les écrits de nos élèves.

« Comme vous pourrez le constater, ces travaux présentent peu de réflexion mathématique, les justifications qu’on peut attendre n’apparaissent pas ; prenez-les comme la véritable production de nos élèves.

« A leur décharge, nous pouvons dire que nous avons fonctionné
• 1 heure par semaine, ce qui est tout-à-fait insuffisant pour le travail en groupe
• avec des élèves issus d’une même classe de Seconde (les sujets n’étant peut-être pas adaptés à eux)
• avec un jumelage qui n’a pas permis un bon échange mathématique (lors des séminaire mais aussi lors de la phase finale, au moment de la rédaction des écrits).

« Ce relatif échec prouvera, si besoin est, que certaines conditions de fonctionnement sont indispensables à la bonne marche d’un projet “MATh.en.JEANS”. »

[NDLR : c’est imparfait mais nous sommes persuadés que c’est utile. Cependant, le texte que les élèves nous ont fourni ne peut être publié tel quel ; nous avons essayé de conserver les idées, en supprimant les passages lisibles par leurs seuls auteurs ; un dernier séminaire, avec les élèves du lycée Jean Jaurès d’Argenteuil, consacré à la rédaction des actes, nous aurait certainement évité l’embarras dans lequel ce texte nous a mis.]

Nous avons trouvé judicieux d’introduire le sujet par un exemple explicite : le 13 octobre 1993 était un mercredi, nous nous sommes posé la question de savoir quel jour serait :

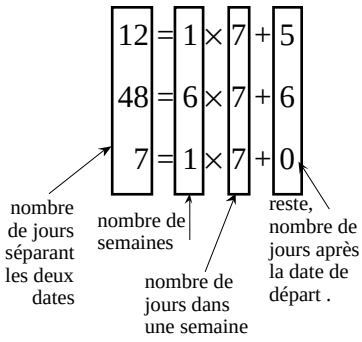
- le 20 octobre 1993 ?
- le 25 octobre 1993 ?
- le 30 novembre 1993 ?

• <u>pour le 20 octobre 1993</u> :
20 - 13 = 7
13 : date de départ ;
7/7 = 1 (1 semaine). Il y a 7 jours dans une semaine. Donc le 20 octobre sera un mercredi, 7 jours après la date de départ.

• <u>pour le 25 octobre 1993</u> :
25 - 13 = 12.
Or 12 = 7 + 5. Nous ne nous occupons que du 5 car le 7 représente une semaine, le jour que nous cherchons se situe alors 5 jours après le mercredi, c’est donc un lundi.

• <u>pour le 30 novembre 1993</u> :
30 + 31 - 13 = 48
30 : date recherchée ;
31: jours du mois d’octobre ;
13 : date de départ ;
48 = (6 × 7) + 6. Nous ne nous occupons que du 6 donc le 30 novembre sera le 6ème jour après le mercredi, donc un mardi.

On remarque que :




Dans ces trois cas, on a réalisé la division euclidienne des nombres 12 puis 48 puis 7 par 7, et ce qui nous intéresse, c’est le reste de la division de ces nombres par 7.

***Définition de la division euclidienne***

Soit $n$ un entier et $N$ un entier différent de 0. Il existe $q$ et $r$ entiers uniques tels que :

$$n = (N \times q) + r \quad \text{et} \quad 0 \leq r \leq N - 1.$$

On peut noter : $n[N] = r$

[NDLR : bonjour les problèmes ! Cette notation est vraiment malcommode, la suite des écrits des élèves étant révélatrice du mal qu'ils eurent à la maîtriser. Nous livrons tout de même au lecteur les extraits les plus lisibles du texte des élèves.]

***Calculs modulo [N]***

Soient $x$ et $y$ deux entiers positifs. Le calcul de $x$ ***modulo*** $y$ s'effectue comme la division euclidienne de $x$ par $y$. Le reste de cette division euclidienne est le résultat du calcul de $x$ modulo $y$.

[NDLC : c'est ***un*** moyen de calcul ; quand j'étais petite, on m'a appris la *preuve par neuf* et on m'a appris aussi des règles de divisibilité par 3 et par 9 ; par exemple, pour savoir si 1994 est divisible par 9, je pouvais faire les calculs de plusieurs façons :

$1 + 9 + 9 + 4 = 23$ ; $2 + 3 = 5 \neq 0$ et 9
$9 \rightarrow 0$ ; $1 + 0 + 0 + 4 = 5 \neq 0$ et 9

mais, bien sûr, on peut *aussi* poser la division euclidienne de 1994 par 9 :

$$1994 = 221 \times 9 + 5,\ 0 \leq 5 \leq 9\text{-}1.$$

Une ***classe*** $r$ modulo $N$ ($r[N]$) est l'ensemble de tous les entiers dont le reste de la division par $N$ est $r$ avec $0 \leq r \leq N - 1$ ; $r$ est appelé le ***plus petit représentant*** de $r[N]$. On dit que deux classes sont ***égales*** si leurs plus petits représentants sont les mêmes. Dans le modulo 9 les études se font sur 9 éléments de 0 à 8.

[NDLC : puisqu'on parle du "modulo 9", d'où vient la *preuve par neuf* ?]

***Propriétés immédiates***

• soit $x$ un nombre quelconque, 1 modulo $x$ est égal à 1 si $x > 1$

• $x$ modulo $y$ est égal à $x$ si $y > x$

• quelque soit le modulo, la classe de 0 n'a pas d'inverse

• dans un modulo de nombre premier, tous les nombres ont un inverse sauf la classe de 0. [NDLR : cette propriété *n'est pas* immédiate.]

• dans un modulo de nombre non premier, tous les nombres ayant un diviseur commun avec le modulo n'ont pas d'inverse. [NDLC : ça, c'est immédiat ?][NDLR : et les nombres n'ayant pas de diviseur commun avec le modulo ?]

Voici quelques petits exemples pour mieux comprendre :

188 = 6[7]  367 = 3[7]
555 = 2[7]  24 = 3[7]
182 = 0[7] (182 est un multiple de 7)
365 = 1[7]

***Addition***

Il faut vérifier que dans les modulos [$N$] :

$$(a + b)[N] = (a[N] + b[N])\ [N]$$

[NDLR : il s'agit de vérifier que l'addition habituelle se transfère aux modulos :]

Prenons un exemple :

$a = 188$ ; $b = 367$ , $N = 7$
$a = \mathbf{6}[7]$, $b = \mathbf{3}[7]$, $\mathbf{6} + \mathbf{3} = 2[7]$
$a + b = 555$, $(a + b) = 2[7]$

[NDLR : donc qu'on prenne 6 ou 188, et qu'on prenne 3 ou 367, l'addition donnera le même résultat modulo 7 et on peut donc faire les calculs autrement qu'en posant la division euclidienne (voir la NDLC, plus haut, à propos de la divisibilité par 9).]

[NDLR : après l'exemple modulo 7, les élèves donnent une démonstration, que leur notation maladroite rend illisible.]

***commutativité*** *:*

[NDLR : il s'agit maintenant de s'assurer du transfert des propriétés classiques de l'addition aux modulos : cette nouvelle opération est-elle aussi commutative, associative, etc ? En résumé, pourra-t-on continuer à calculer comme on a l'habitude de le faire, ou non ? Exemple :]

*a*=188, *b*=367. Pour *N* = 7, on obtient :

$$(188 + 367)\,[7] = (3[7] + 6[7])\,[7]$$
$$(367 + 188)[7] = 2[7]$$

[NDLR : après la commutativité, on passe à l'associativité de l'addition, puis à la multiplication.]

*Opérations modulo 7 : addition et multiplication, les tables :*

**ADDITION**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | *0* | *1* | *2* | *3* | |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | *7* | *8* | *9* | *10* ... |
| 0 | **0** | **1** | **2** | **3** | **4** | **5** | **6** | *0* | *1* | *2* | *3* |
| 1 | **1** | **2** | **3** | **4** | **5** | **6** | **0** | *1* | *2* | *3* | *4* |
| 2 | **2** | **3** | **4** | **5** | **6** | **0** | **1** | *2* | *3* | *4* | *5* |
| 3 | **3** | **4** | **5** | **6** | **0** | **1** | **2** | *3* | *4* | *5* | *6* |
| 4 | **4** | **5** | **6** | **0** | **1** | **2** | **3** | *4* | *5* | *6* | *0* |
| 5 | **5** | **6** | **0** | **1** | **2** | **3** | **4** | *5* | *6* | *0* | *1* |
| 6 | **6** | **0** | **1** | **2** | **3** | **4** | **5** | *6* | *0* | *1* | *2* |

**MULTIPLICATION**

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | **0** | **0** | **0** | **0** | **0** | **0** | **0** |
| 1 | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| 2 | **0** | **2** | **4** | **6** | **1** | **3** | **5** |
| 3 | **0** | **3** | **6** | **2** | **5** | **1** | **4** |
| 4 | **0** | **4** | **1** | **5** | **2** | **6** | **3** |
| 5 | **0** | **5** | **3** | **1** | **6** | **4** | **2** |
| 6 | **0** | **6** | **5** | **4** | **3** | **2** | **1** |

[NDLR, pour le lecteur : une fois ces règles de calcul mises en place, il reste à voir ce qu'on peut en faire … à vous. Voir aussi l'article de Jean-Paul Cardinal, page 231.]

[NDLR, pour la claviste : la *preuve par neuf* consiste à remplacer la multiplication qu'on cherche à effectuer par la multiplication des classes modulo 9, et à comparer avec la classe modulo 9 du résultat obtenu. Exemple pour l'opération 1994 × 365 effectuée à la main : 1994 est dans la classe de 5 modulo 9 ; 365 est aussi dans la classe de 5 modulo 9 ; au lieu d'effectuer 1994 × 365, on effectue 5× 5, on obtient 25, qui est dans la classe de 7 modulo 9. Si le résultat trouvé en effectuant 1994 × 365 à la main n'est pas dans la classe de 7 modulo 9, c'est qu'il y a eu erreur de calcul. On devrait trouver 727810 ; si on trouve 72781, ou 720160, ou …, la preuve par neuf ne voit pas l'erreur de calcul ; si on trouve 727910, elle la verra. On espère que la claviste a compris.] [NDLC : ça peut aller.]

[NDLR : voir aussi l'article "142857" et son annexe sur Z/*DZ*, page 192, à lire au niveau fin de T^le^, ou *maths sup*.]