

Division, modulo et clefs de contrôle

Soient n , p et k trois entiers. On dit que « n est égal à p modulo k », et on note $n = p [k]$, si $n - p$ est divisible par k . Autrement dit, $n = p [k]$ si et seulement si $n = p + q \times k$ avec q un entier. Voici quelques propriétés importantes à retenir :

- il existe un unique entier p entre 0 et $k - 1$ tel que $n = p [k]$ et p est alors le reste de la division euclidienne de n par k . Calculer p se dit souvent « calculer n modulo k ».
- n est divisible par k si et seulement si $n = 0 [k]$.
- si $n = p [k]$ et $n' = p' [k]$, alors $n + n' = p + p' [k]$, $n - n' = p - p' [k]$ et $nn' = pp' [k]$.

Exercice : Calculer $96 [7]$ et $135 [4]$. Vérifier que $100 [7]$ est bien égal à $(10 [7]) \times (10 [7])$ modulo 7.

Critères de divisibilité

Calculer $10 [9]$, $100 [9]$, $1000 [9]$ et plus généralement $10^i [9]$. Montrer que

$$\overline{a_n a_{n-1} \dots a_3 a_2 a_1} [9] = a_n + a_{n-1} + \dots + a_3 + a_2 + a_1 [9] .$$

En déduire le critère de divisibilité par 9. Montrer de même le critère de divisibilité par 3. Montrer qu'un nombre $\overline{a_3 a_2 a_1}$ est divisible par 7 si et seulement si $a_1 + 3a_2 + 2a_3$ est divisible par 7.

Clefs d'un code

Dans la vie courante, on utilise souvent des nombres pour coder ou inventorier des objets. Il est souvent important de ne pas se tromper en les écrivant (par exemple pour le code RIB lors d'un virement !). Or, certaines erreurs sont malheureusement courantes :

- omission d'un chiffre,
- erreur sur un chiffre durant la saisie,
- inversion de deux chiffres consécutifs.

S'il est facile de vérifier automatiquement que le nombre de chiffres est correct, les autres erreurs sont plus difficiles à détecter. Pour ce faire, on ajoute au code une « clef » qui consiste en un ou deux chiffres supplémentaires. Ces chiffres sont reliés au code par une formule et on peut vérifier si l'ensemble code+clef correspond à un ensemble pertinent ou s'il n'est pas correct (erreur de saisie quelque part).

La clef la plus simple consiste à calculer le code n modulo un chiffre k . Par exemple, si la clef se calcule modulo 6, le code 4518 a pour clef 0 et on le note désormais 4587 0.

1) On suppose encore que la clef se calcule modulo 6. Donner la clef du code 2387.

On cherche dorénavant le chiffre k pour que la clef modulo k soit la plus efficace pour détecter les erreurs de saisie.

- 2) Que pensez-vous de la clef modulo 2 ? En quoi n'est-elle pas efficace ?
- 3) Quels chiffres divisent 10, 100, 1000 ou une autre puissance de 10 ? Pourquoi ne doit-on pas les choisir pour calculer la clef ?
- 4) Pourquoi ne pas prendre $k = 3$ ou $k = 9$?
- 5) Donner un critère de division par 6. Montrer que $k = 6$ ne fournit pas une clef très robuste.
- 6) Le chiffre $k = 7$ paraît donc le meilleur candidat. Toutefois, il n'est pas parfait. En effet, montrer qu'il existe deux nombres différents \overline{ab} et \overline{ba} qui ont la même clef modulo 7.

Clef du numéro de sécurité sociale

Un numéro de sécurité sociale se décompose ainsi :

1	72	10	38	314	159	42
sexe	année de naissance	mois de naissance	département de naissance	commune de naissance	numéro d'inscription	clef

NB : ce numéro est un numéro fictif.

La clef du numéro se calcule comme suit. On considère tout ce qui précède comme un nombre à 13 chiffres, on calcule le reste p de ce nombre modulo $k = 97$ et la clef est alors $97 - p$.

A votre avis, quelle est la particularité de 97 qui a poussé à ce choix ? Montrer que le calcul de la clef modulo 97 permet de détecter toutes les erreurs simples de saisie¹.

Pour vérifier la clef de l'exemple ci-dessus, il faudrait une calculatrice gérant les nombres à 13 chiffres, ce qui n'est pas évident. Pour faire plus simple, montrer que $100 = 3 [97]$ et donc que $1\,000\,000 = 27 [97]$. En déduire que la clef se trouve par le calcul $1721038 \times 27 + 314159 [97]$ et vérifier que le numéro ci-dessus a bien été saisi.

Clef du numéro ISBN

Les livres sont référencés en France par leur numéro ISBN qui se présente ainsi :

2	-	070	-	41239	-	3
pays (francophone)		éditeur (Gallimard)		livre (<i>Le rouge et le noir</i>)		clef

La clef du code $a_1 - a_2a_3a_4 - a_5a_6a_7a_8a_9$ est obtenue par le calcul

$$\text{clef} = a_1 + 2a_2 + 3a_3 + 4a_4 + \dots + 9a_9 [11] ,$$

où le résultat est soit un nombre entre 0 et 9, soit le symbole x si le reste modulo 11 est 10.

Vérifier que le code ci-dessus est correct. Montrer que la clef du code ISBN permet de détecter les erreurs de saisie classiques¹.

1. Attention, question difficile, que l'on pourra passer en première lecture