Exemples de clés de contrôle

Lors de la saisie d'un numéro, les trois types d'erreur les plus fréquents sont :

- **un chiffre erroné**
- **erreur dans le nombre de chiffres**
- **permutation de deux chiffres.**

On introduit donc une clé de contrôle susceptible de mettre en évidence certaines erreurs de saisie.

Numéro ISBN **Ce numéro comporte 9 chiffres identifiant la langue de publication, l'éditeur, le numéro de l'ouvrage, : $a_1a_2\ldots a_9$, suivis d'une clé de contrôle comprenant un seul chiffre : C**

On calcule le reste r le reste de la division par 11 du nombre
$a_1 + 2a_2 + 3a_3 + \ldots\ldots\ldots + 9\,a_9$.
si r < 10 alors C = r
si r = 10 alors C = X

Cette clé permet-elle de repérer les principales erreurs de saisie ?

Si N et N' sont deux numéros qui *différent par leur* $k^{ième}$ *chiffre*
$N' - N = (a'_k - a_k)\times 10^k$ avec k et $(a'_k - a_k)$ dans {1, 2, …, 9}

clé(N') –clé(N) = $k\times(a'_k - a_k)$ est premier avec 11
clé(N') –clé(N) ≠0.

Si N et N' sont deux numéros qui diffèrent *par interversion des chiffres* a_i *et* a_j

clé N' – clé N= $i\times a_i + j\times a_j - (j\times a_i + i\times a_j) = (a_i - a_j)(i - j)$

$(a_i - a_j) \in \{1, 2, \ldots.., 9\}$ et $(i - j) \in \{1, 2, \ldots.., 9\}$ donc
$(a_i - a_j)(i - j)$ est premier avec 11.

clé N' – clé N ≠ 0

en particulier, pour deux numéros consécutifs, clé N' – clé N= $(a_{i+1} - a_j)$

Codes barres

Douze chiffres $a_1a_2\,a_3\ldots..a_{11}\,a_{12}$ identifiant le pays, le fournisseur, le produit, et un chiffre clé C.
Calcul de la clé :
On calcule les sommes
$S = a_{12} + a_{10} + a_8 + a_6 + a_4 + a_2$ et $S' = a_{11} + a_9 + a_7 + a_5 + a_3 + a_1$

$C \equiv 10 - (3\times S + S')$ modulo 10

Numéro INSEE **Ce numéro comporte 13 chiffres : $a_1a_2\ldots a_{13}$ suivis d'une clé de contrôle comprenant un ou deux chiffres : C**

On calcule le reste r de la division de $a_1a_2\ldots a_{13}$ par 97 . $C = 97 - r$
donc **$C \equiv 97 - a_1a_2\ldots a_{13}$ modulo 97**

Le calcul de la clé de contrôle INSEE n'est plus possible avec les outils de calcul classiques, compte tenu de la taille des nombres. Il est nécessaire de morceler le calcul, en travaillant sur des restes partiels.

En notant A et B les nombres écrits avec les 7 premiers ou les 6 derniers chiffres de N, on a :
$N = A \times 10^6 + B$.
En divisant A, B, 10^6 par 97, on obtient :
$A = 97q_A + r_A$, $0 \leq r_A \leq 96$,
$B = 97q_B + r_B$, $0 \leq r_B \leq 96$
$10^6 = 97q_0 + r_0$, $0 \leq r_0 \leq 96$.

$N = A \times 10^6 + B = (97q_A + r_A).(97q_0 + r_0) + 97q_B + r_B$ donc $N = 97(Q) + r_A.r_0 + r_B$.

$N \equiv 97 - (r_A.r_0 + r_B)$ modulo 97

***Le calcul du reste de* $r_A.r_0 + r_B$ *modulo* 97 *est devenu possible avec les outils classiques puisque ce nombre est inférieur ou égal à* $96 \times 97 = 9312$.**

On définira donc la notion de congruence modulo p

Soit a et b deux entiers relatifs,

a et b sont congrus modulo p si et seulement si b – a est multiple de p. **qu'on écrira : $a \equiv b$ modulo p.**

Quelques propriétés simples seront établies :

$a \equiv b$ modulo p si et seulement si b et a le même reste dans la division euclidienne par p.

soit **r le reste de la division euclidienne de a par p**,
alors **$a \equiv r$ modulo p**

quelques "règles opératoires":

transitivité:

si $a \equiv b$ modulo p et si $b \equiv c$ modulo p **alors $a \equiv c$ modulo p**

compatibilité avec l'addition ou la multiplication:

si $a \equiv b$ modulo p et si $a' \equiv b'$ modulo p
alors $a + a' \equiv b + b'$ modulo p
et $a \times a' \equiv b \times b'$ modulo p

Applications:

Clé INSEE

Définition de la clé INSEE : $C \equiv 97 - N$ modulo 97, $0 \leq C \leq 96$

Calcul de la clé INSEE : $C \equiv 97 - (r_A . r_0 + r)$ modulo 97, $0 \leq C \leq 96$

Repérage des erreurs :

Si N *et* N' sont deux entiers qui *différent par leur* $k^{ième}$ *chiffre*

$N' - N = (a'_k - a_k) \times 10^k$, k et (a'– a) dans {1, 2, …, 9}

clé(N') –clé(N) $\equiv (a'_k - a_k) \times 10^k$ (mod 97)
97 est premier. Il ne divise ni $(a'_k - a_k)$ ni 10^k donc 97 ne divise pas $(a'_k - a_k) \times 10^k$
clé(N') –clé(N) ≠0.

Si N *et* N' sont deux entiers qui *différent par interversion des chiffres* a_i *et* a_j

$N' - N = (a_i - a_j) \times 10^i \times (10^j - 1)$,
i et j dans{1, 2, …, 9}et (a'– a) dans {1, 2, …, 9}
$(a_i - a_j) \in$ {1, 2, ….., 9}, i et j dans {1, 2,.., 12}

97 ne divise ni $(a_i - a_j)$ ni 10^i ni $(10^j - 1)$, donc 97 ne divise pas N' – N.
clé N' – clé N ≠ 0

Calcul du reste r_n modulo p de a^n, a et p étant deux entiers naturels.

$r_0 = 1$ et
pour tout entier naturel k, $a^k \equiv r_k$ modulo p donc $a_{k+1} \equiv a \times r_k$ modulo p donc
$r_{k+1} \equiv a \times r_k$ modulo p

Le reste modulo p de $a \times r_k$, est donc le reste de a^{k+1} modulo p.

De proche en proche, on pourra calculer le reste modulo p de n'importe quelle puissance de a.

Ce calcul peut être proposé sur le tableur.
On pourra observer que pour p premier et a non multiple de p, ces restes sont périodiques (dans ce cas, $a^{p-1} \equiv 1$ modulo p)

CRITERE DE DIVISIBILITE PAR P

Soit p entier supérieur ou égal à 2.

Soit N un entier $N = \sum_{k=0}^{n} a_k.10^k$

Pour tout entier naturel k, $10^k \equiv r_k$ modulo p donc $N \equiv \sum_{k=0}^{n} a_k.r_k$ modulo p .

N et $\sum_{k=0}^{n} a_k.r_k$ **ont même reste dans la division par p**.

N divisible par p si et seulement si $\sum_{k=0}^{n} a_k.r_k \equiv 0 \pmod p$

Remarque:

dans tous les cas on obtient le reste de N modulo p.

EXEMPLES

$p = 2^i$ ou $p = 5^i$

Pour tout $k \geq i$, $r_k = 0$ $\quad N \equiv \sum_{k=0}^{i} a_k.r_k$ modulo p.

Pour $p = 2^i$ ou $p = 5^i$ N est divisible par p si et seulement si le nombre dont l'écriture décimale est constituée par les i derniers chiffres de N est lui-même divisible par p.

p = 3 ou p = 9

$10 \equiv 1 \pmod p$, donc pour tout $k \geq 1$, $10^k \equiv 1 \pmod p$

pour tout $k \geq 1, r_k = 1$ donc $\mathbf{N \equiv \sum_{k=0}^{i} a_k}$ **modulo p**.

Pour p = 3 ou p = 9,
reste de N modulo p = reste modulo p de la somme des chiffres de N.

Pour p = 3 ou p = 9, N est divisible par p si et seulement si la somme des chiffres de N est elle-même divisible par p.

p = 11

$10 \equiv -1$ modulo 11. Donc

pour k pair, $10^k \equiv 1 \pmod{11}$, $r_k = 1$

pour k impair, $10^k \equiv -1 \pmod{11}$, $r_k = -1$

$N \equiv \sum_{k=0}^{i} (-1)_k . a_k$ modulo p .

N est divisible par 11 si et seulement si la somme alternée des chiffres de n est divisible par 11.

PREUVE PAR NEUF

Peut-on vérifier l'exactitude des opérations suivantes

- **3486×12481 = 43508766 ?**

3486 ≡ 3 modulo 9 et 12481 ≡ 7 modulo 9

Donc 3486×12481 ≡ 3×7 (mod 9) ≡ 3 (mod 9)

Or 43508766 ≡ 3 (mod 9). **On n'a pas repéré d'erreur** (l' opération est exacte).

- **23449457 = 3251×7213 + 4 ?**

3251 ≡ 2 (mod 9) et 7213 ≡ 4 (mod 9)

3251×7213 + 4 ≡ 2×4 + 4 (mod 9) ≡**3 (mod 9).**

Or 2 + 3 + 4 + 4 + 9 + 4 + 5 + 7 ≡ 2 (mod 9).
23449457 ≡ 2 (mod 9). L'opération est erronée et l'erreur est repérée.

- **9009 = 63×142 ?**

9009 ≡ 0 (mod 9), 63 ≡ 0 (mod 9)

donc 63×142 ≡ 0 (mod 9)

Or 63×142 = 8946. L'erreur n'a pas été repérée par comparaison des restes modulo 9 car
9009 = 8946 + 63 donc 9009 ≡ 8946 modulo 9

La comparaison des restes modulo 9 ne permet pas de repérer une telle erreur.

Utilisation du tableur pour le calcul de clés

	B	C	D	E	
2					
3			clé INSEE	38	
4		q			
5		97			
6					
7		Numéro	sept premiers	six derniers	
8		1430467482127	chiffres	chiffres	
9			1430467	482127	
10					
11			8	37	
12					

D9 : = STXT(C8 ; 1 ; 7) **E9: = STXT(C8 ; 9 ; 6)**

D11 : = MOD(D9; 97) **E11 : = MOD(E9; 97)**

E3 : = MOD(10^6×D11 + E11; 97)

	B	C	D	E	F	G	H	I	J
2									
3		Clé	3						
4									
5									
6		rang	12	10	8	6	4	2	
7	Code barre	chiffre	0	0	0	2	8	0	10
8	306832004010								
9		rang	11	9	7	5	3	1	
10		chiffre	1	4	0	3	6	3	17

Cellules D7 à I7 : = STXT(B8 ; X7 ;1)
Cellules D10 à I10 : = STXT(B10 ; X10 ;1)

Cellule J7 : = SOMME (D7 :I7)
Cellule J10: = SOMME (D10 :I10)

Cellule D3 : = 10 - MOD(3*J7 + J10 ; 11)

Exemples d'applications

Calculs de clés (feuille de calcul EXCEL)
Code barre : N = 9 78270962048

S = 8 + 0 + 6 + 0 + 2 + 7 = 23 et S' = 4 + 2 +9 + 7 + 8 + 9 = 39
3 S + S' = 108 Clé = 2

Code ISBN: N = 270962048

$2 + 2\times7 + 3\times0 + 4\times9 + 5\times6 + 6\times2 + 7\times0 + 8\times4 + 9\times8 = 198 = 18\times11.$ Clé = 0

Compléter le numéro INSEE : 1 75 11 3 x 162 235 68

R = 97 – 68 = 29
$29 \equiv 1751130162235 + x.10^6 \pmod{97}$
$162235 \equiv 51 \pmod{97}$
$1751130 \equiv 86 \pmod{97}$ et $10^6 \equiv 27 \pmod{97}$
$1751130\,162235 \equiv 86 \times 27 + 51 \pmod{97} \equiv 45 \pmod{97}$

Donc $45 + 27x \equiv 29 \pmod{97}$
$27x \equiv 29 - 45 \pmod{97} \equiv -16 \pmod{97} \equiv 81 \pmod{97}$ x = 3

Vérifier le numéro INSEE : 2 34 07 56 235 123 23
Proposer une correction, sachant que la clé est correcte.

Recherche du jour de la semaine correspondant à une date donnée
(feuille de calcul EXCEL)

0 correspond au dimanche, 1 correspond au lundi, …….
q désigne le quantième du mois
mois désigne le n° du mois (janvier 1, février 2,…)
année correspond au millésime de l'année, avec tous ses chiffres.

En notant [x] la partie entière du réel x,
c = $\left\lfloor \frac{14-\text{mois}}{12} \right\rfloor$ c est donc égal à 0 ou à 1.

a = année – c et m = mois + 12 c – 2.

$j \equiv q + a + \left\lfloor \frac{a}{4} \right\rfloor - \left\lfloor \frac{a}{100} \right\rfloor + \left\lfloor \frac{a}{400} \right\rfloor + \left\lfloor \frac{31m}{12} \right\rfloor \pmod{7}$

Exemple:

Quel jour de la semaine tombera le 25 décembre 2002?

$q = 25$, $c = \left\lfloor \frac{14-12}{12} \right\rfloor = 0$, $a = 2002 - 0$, $m = 12 + 12 \times 0 - 2$

$j \equiv 25 + 2002 + 500 - 20 + 5 + 25 \pmod 7$

$j = 3$ donc le 25 décembre 2002 sera un mercredi.

Quel jour de la semaine était le 1er janvier 2001 ?

$q = 1$, $c = \left\lfloor \frac{14-1}{12} \right\rfloor = 1$, $a = 2001 - 1$, $m = 1 + 12 \times 1 - 2$

$j \equiv 1 + 2000 + 500 - 20 + 5 + 28 \pmod 7$

$j = 1$ donc le 1er janvier 2001 était un lundi.