LYCÉE ALFRED KASTLER **TS-spé**
2011–2012

Devoir maison n°01 – mathématiques
Correction

Question d) de l'exercice 157p32
On commence par démontrer la propriété suivante :

Propriété Soit a et b deux entiers. Soit d un entier. Les nombres a et $a+b$ ont le même reste dans la division euclidienne par d si et seulement si d divise b (autrement dit le reste de la division euclidienne de b par d vaut 0).

Preuve : Dans toute la preuve on note les égalités suivante :

$$a = q_a \times d + r_a \quad ; \quad b = q_b \times d + r_b \quad \text{et} \quad a + b = q \times d + r$$

où r_a, r_b et r sont des entiers positifs strictement inférieurs à d.

- On suppose que a et $a+b$ ont le même reste dans la division euclidienne par d. On a donc $r_a = r$, et on souhaite prouver que $r_b = 0$.
  Or $a + b = q \times d + r_a$ mais aussi $a + b = q_a \times d + r_a + q_b \times d + r_b = (q_a + q_b) \times d + r_a + r_b$. Ainsi,

$$\begin{aligned} & q \times d + r_a = (q_a + q_b) \times d + r_a + r_b \\ \Leftrightarrow \quad & (q - q_a - q_b) \times d = r_b \end{aligned}$$

  Ce qui signifie que d divise r_b. Or $0 \leq r_b < d$, donc nécessairement $r_b = 0$
- On suppose réciproquement que d divise b. On a alors $r_b = 0$ et on souhaite prouver que $r_a = r$.
  Or $a + b = q_a \times d + r_a + q_b \times d = (q_a + q_b) \times d + r_a$, et $0 \leq r_a < d$. Donc r_a est le reste de la division euclidienne de $a + b$ par d. Autrement dit, $r_a = r$. □

On considère le nombre A définit dans l'énoncé de l'exercice. On suppose que l'on modifie un chiffre et un seul dans A. On obtient alors un nombre $A' = A + e$ (ou $A' = A - e$)$^{(\star)}$ avec $e = c \times 10^n$, $1 \leq c \leq 9$ et $0 \leq n \leq 13$.
On veut démontrer qu'alors l'erreur est détectée, c'est à dire que que la clé correspondant à A est différente de la clé correspondant à A'.
Pour cela il suffit de prouver que le reste de la division euclidienne de A par 97 est différent du reste de la disivion euclidienne de $A + e$ (ou $A - e$) par 97.
D'après la propriété ci-dessus, il suffit de prouver que e (ou $-e$, ce qui revient ici au même) n'est pas divisible par 97.
Or, 97 est un nombre premier. Ce qui signifie que 97 divise e si et seulement si 97 apparaît dans la décomposition en produit de nombres premiers de e (e est non nul).
Or $e = c \times 10^n = c \times 2^n \times 5^n$, avec $1 \leq c \leq 9 < 97$: 97 n'apparaît dans la décomposition de e.

On a donc bien démontré que l'erreur est détectée. En fait, pour que l'erreur ne soit pas détectée, il suffit (et c'est nécessaire) d'ajouter à A un multiple de 97, ce qui se fait difficilement involontairement du fait que 97 est premier.

Finalement, il a été inutile d'utiliser la méthode proposée.

$^{(\star)}$ On peut voir la modification d'un chiffre comme l'augmentation ou la diminution d'un des chiffres du nombre à 13 chiffres.