ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

SCIENCES DE L'INFORMATION

Série 6

Olivier Cloux

6.1

1. • Décomposition de 68 : $\begin{array}{r|l} 68 & 2 \\ 34 & 2 \\ 17 & 17 \\ 1 & \end{array} \rightarrow \boxed{68 = 2^2 \cdot 17}$

   • Décomposition de 187 : $\begin{array}{r|l} 187 & 11 \\ 17 & 17 \\ 1 & \end{array} \rightarrow \boxed{187 = 11 \cdot 17}$

   • Décomposition de 176 : $\begin{array}{r|l} 176 & 2 \\ 88 & 2 \\ 44 & 2 \\ 22 & 2 \\ 11 & 11 \\ 1 & \end{array} \rightarrow \boxed{176 = 2^4 \cdot 11}$

2. Le *pgcd* de deux nombres se calcul en multipliant tous les facteurs premiers en commun dans la décomposition de ces deux nombres, à leur plus faible puissance
   - $pgcd(68, 187) = 17 = \boxed{17}$
   - $pgcd(68, 176) = 2^2 = \boxed{4}$
   - $pgcd(176, 187) = 11 = \boxed{11}$

3. Deux nombres sont premiers entre eux si leur *pgcd* est de 1. Comme nous l'avons calculé, aucun des *pgcd* n'est de 1, donc *de facto*, ni *a,b*, ni *a,c* ni *b,c* ne sont premiers entre eux.

4. Nous savons que

$$\begin{aligned} ab \mod p &= 0 \\ (a \mod p)(b \mod p) \mod p &= 0 \end{aligned}$$

Par définition, pour tout entier k, $0 \leq (k \mod p) < p$.
En supposons que p ne divise ni a ni b, nous savons que:

$$(a \mod p) \neq 0 \text{ et } (b \mod p) \neq 0$$

En sachant cela, il devient impossible que $(a \mod p)(b \mod p) = 0$. De plus, comme p est premier, il n'existe pas deux entiers (différents de 1 et p) qui multipliés donnent p. Cela fait que $(a \mod p)(b \mod p) \neq p$.
Avec ces deux affirmations, nous n'aurons jamais $(a \mod p)(b \mod p) \mod p = 0$.

En revanche, si uniquement a est divisible par p, alors $(a \mod p) \equiv 0 \mod p$, donc $0 \cdot (b \mod p) = 0 \ \forall b$. Nous pouvons généraliser notre postulat à "seulement b est divisible par p" (car $(a \mod p) \cdot 0 \equiv 0 \mod p \ \forall a$) et à "$a$ <u>et</u> b sont divisibles par p"(car $0 \cdot 0 \equiv 0 \mod p$).

En d'autres mots, <u>soit p divise a, soit p divise b (ou les deux)</u>.

6.2

1. En appliquant les règles sur le modulo :

$$\begin{aligned}
& 12345678901234578901234567111 \mod 1000 \\
= \ & (1234567890123456789012345670000 + 111) \mod 1000 \\
= \ & \big((1234567890123456789012345670000 \mod 1000) + (111 \mod 1000)\big) \mod 1000 \\
= \ & \big(0 + 111) \mod 1000 \\
= \ & \boxed{111}
\end{aligned}$$

2. Rappelons qu'un chiffre à une puissance paire devient positif, alors qu'à une puissance impaire il reste négatif.

   Rappelons également que $(a^x \mod p) = ((\overbrace{a \cdot a \cdot a \cdot ... \cdot a}^{\times x}) \mod 7)$
   $= (\overbrace{(a \mod p) \cdot (a \mod p) \cdot \ldots \cdot (a \mod p)}^{\times x}) \mod p = ((a \mod p)^x \mod p)$

   Enfin, x est multiple de $p \iff x \equiv 0 \mod p$.

   - a :
   $$\begin{aligned}
   & (48^{12345678901234567890} + 69^{98765432109876543211} + 2) \mod 7 \\
   = \ & ((48^{12345678901234567890} \mod 7) + (69^{98765432109876543211} \mod 7) + (2 \mod 7)) \mod 7 \\
   = \ & ((-1)^{12345678901234567890} + (-1)^{98765432109876543211} + 2) \mod 7 \\
   = \ & (1 - 1 + 2) \mod 7 = 2 \mod 7 = \boxed{2}
   \end{aligned}$$
   $\rightarrow a$ n'est <u>pas</u> un multiple de 7.

   - b :
   $$\begin{aligned}
   & (34^{12345678901234567890} + 69^{9876543210} + 4) \mod 7 \\
   = \ & ((34^{2345678901234567890} \mod 7) + (69^{9876543210} \mod 7) + (4 \mod 7)) \mod 7 \\
   = \ & (1^{12345678901234567890}) + (-1)^{9876543210} + 4) \mod 7 \\
   = \ & (1 + 1 + 4) \mod 7 = 6 \mod 7 = \boxed{6}
   \end{aligned}$$
   $\rightarrow b$ n'est <u>pas</u> un multiple de 7.

   - c :
   $$\begin{aligned}
   & 37^{9876543} \mod 7 \\
   = \ & 2^{9876543} \mod 7 \\
   = \ & (2^3)^{\frac{9876543}{3}} \mod 7 = (2^3)^{3292181} \mod 7 \\
   = \ & 8^{3292181} \mod 7 = 1^{3292181} \mod 7 = 1 \mod 7 = \boxed{1}
   \end{aligned}$$
   $\rightarrow c$ n'est <u>pas</u> (non plus) un multiple de 7.

6.3

1. (a) $x_{13} = -\big(9+8+4+9+1+9+3\cdot(5+1+3+8+9+2)\big) \mod 10 = \boxed{6}$
   (b) $x_{13} = -\big(1+3+5+7+9+9+3\cdot(2+4+6+8+0+8)\big) \mod 10 = \boxed{2}$
2. Il faut s'assurer que

$$x_{13} = -\Big(x_1 + x_2 + x_3 + \ldots + x_{11} + 3\cdot(x_2 + x_4 + \ldots + x_{12})\Big) \mod 10$$

   Si le dernier chiffre ne correspond pas à cette équation, alors le numéro ISBN n'est pas valide.

   Notons que nous pouvons aussi vérifier, de manière équivalente, que

$$x_1 + x_3 + ... + x_{11} + x_{13} + 3\cdot(x_2 + x_4 + x_6 + ... + x_{12}) \equiv 0 \mod 10$$

3. (a) $-\big(4+4+4+4+4+4+3\cdot(5+5+5+5+5+5)\big) \mod 10 \stackrel{?}{=} 1$? Non, car c'est égal à 6. Ce numéro ISBN n'est donc pas valide
   (b) $-\big(1+3+8+1+3+8+3\cdot(2+7+9+2+7+9)\big) \mod 10 \stackrel{?}{=} 5$? Non, car c'est égal à 8. Ce numéro ISBN n'est donc pas valide (non plus).
4. Comme nous inversons un chiffre de position paire avec un chiffre de position impaire, il est fort probable que les deux numéros de contrôle diffèrent. En effet, nous n'additionneront plus les mêmes chiffres (à la fois dans la partie paire et la partie impaire). Afin de nous en convaincre, nous n'avons qu'à vérifier par le calcul :
   Dans le cas non-inversé :

$$x = -\big(9+8+4+9+4+9+3\cdot(7+1+3+8+9+2)\big) \mod 10 = 7$$

   Dans le cas inversé :

$$x = -\big(9+8+\underline{3}+9+4+9+3\cdot(7+1+\underline{4}+8+9+2)\big) \mod 10 = 5$$

   Cela vient confirmer nos hypothèses : il n'est pas évident pour une inversion de deux chiffres de parités différentes de changer le numéro de contrôle. Ainsi, cette inversion précise ne donne pas un numéro ISBN valide
5. Il est évident que le ce numéro ISBN est valide : en effet, nous inversons deux chiffres de même parité. Dans notre équation, cela aura pour effet de changer $[...]+4+9+[...]$ en $[...]+9+4+[...]$, ce qui n'influe en rien la valeur du chiffre de contrôle, et donc la validité du numéro. Ce numéro ISBN est donc valide.
6. Afin de trouver un nombre possédant deux chiffres consécutifs tels qu'une fois inversés ne modifient pas le chiffre de contrôle, nous devons appliquer de l'arithmétique modulaire, en posant (pur faciliter la lecture), les variables suivantes:
   Soit k la somme des chiffres de positions impaires non inversés
   Soit m la somme des chiffres de positions paires non-inversés
   Soit x le premier chiffre (de position impaire) inversé
   Soit y le second chiffre (de position paire) inversé
   Nous avons alors que

$$\begin{aligned} x_{13} &= -(x_1 + x_3 + ... + x_{11} + 3\cdot(x_2 + x_4 + ... + x_{12})) \mod 10 \\ &= -(k + x + 3\cdot(m + y)) \mod 10 \end{aligned}$$

   Nous cherchons un donc un x et un y tels que leurs x_{13} respectifs ne diffèrent pas. Notons que tant que la parité est respectée, leur position initiale ne change pas ; autrement dit, x pourrait aussi bien être x_1 que $x_3, x_5, ..., x_{11}$, alors que y pourrait être tant bien x_2 que $x_4, x_6, ..., x_{12}$. Ainsi, nous voulons que

$$(-k - x - 3m - 3y) \mod 10 = (-k - y - 3m - 3x) \mod 10$$

Nous pouvons appliquer sur cette équation les opérations standards, à l'exception de la division (ou de la multiplication par un réel non-entier). Nous trouvons donc :

$$\begin{aligned}
(-k - x - 3m - 3y) \mod 10 &= (-k - y - 3m - 3x) \mod 10 \quad &| + k + 3m\\
(-x - 3y) \mod 10 &= (-y - 3x) \mod 10 \quad &| + x + y\\
(-2x) \mod 10 &= (-2y) \mod 10 \quad &| \times (-1)\\
2x \mod 10 &= 2y \mod 10
\end{aligned}$$

Nous devons donc trouver deux chiffres tels qu'une fois multipliés par 2, leurs mod 10 s'égalent. Par nous pouvons par exemple prendre 3 et 8 (car $6 \mod 10 = 16 \mod 10 = 6$). Les autre chiffres n'importent pas, comme nous l'avons montré il y a un instant. Nous pouvons donc choisir, par exemple, les numéros ISBN $\boxed{\text{15274}\underline{\text{83}}\text{17238 et 15274}\underline{\text{38}}\text{17238}}$, dont les chiffres de contrôle sont les deux “7”.

Comme nous l'avons dit plus haut, on ne peut détecter une erreur/inversion *si et seulement si* le numéro ISBN n'est pas valide, donc si le chiffre de contrôle ne correspond pas à la formule donnée. Par déduction, comme nous avons créé une inversion telle qu'elle n'influence pas le chiffre de contrôle, le système de contrôle est <u>incapable de détecter cette erreur</u>.