M1MI2016 Codes et Cryptologie

Corrigé du DS n° 1 (2012/2013).

Exercice 1

1. Si Bob a reçu 249, c'est que la date x d'Alice vérifie $57x + 44 = 249 \bmod 365$, soit $57x = 205 \bmod 365$. Pour calculer x on doit décider si 53 est inversible modulo 365, et le cas échéant calculer son inverse, et pour cela on applique l'algorithme d'Euclide étendu.

r_k	u_k	v_k	q_k	
365	1	0		
57	0	1	6	$(365 = 57 * 6 + 23)$
23	1	-6	2	$(57 = 23 * 2 + 11)$
11	-2	13	2	$(23 = 11 * 2 + 1)$
1	5	-32		

   Le pgcd de 365 et 57 est égal à 1 donc 57 est inversible modulo 365 et on a la relation de Bezout : $5 * 365 - 32 * 57 = 1$ qui montre que $57^{-1} = -32 \mod 365$. Donc on peut calculer $x = -32 * 205 = 10 \bmod 365$. La date d'Alice est donc le 11 janvier.

2. Dans le cas général, l'équation $ax + b = y \bmod 365$ d'inconnue x a une solution unique si et seulement si a est inversible modulo 365, c'est du cours. Cette solution est alors $x = a^{-1}(y - b) \bmod 365$. Donc Bob peut déchiffrer correctement les messages d'Alice si a est inversible modulo 365, c'est-à-dire si a est premier à 365. La fonction de déchiffrement est $y \mapsto a^{-1}(y - b) \bmod 365$.

3. Si Bob reçoit 221, c'est que $55x+1 = 221 \bmod 365$, soit $55x = 220 \bmod 365$. Mais 55 n'est pas premier à 365, en fait leur pgcd vaut 5. Mais 5 divise 220 donc $55x = 220 \bmod 365$ si et seulement si $11x = 44 \bmod 73$ (vu en cours). Il reste à inverser 11 modulo 73 et pour cela on applique Euclide étendu, et on trouve $11^{-1} = 20 \bmod 73$. Donc $x = 20*44 = 4 \bmod 73$. Il reste à remonter aux solutions modulo 365 :

$$\begin{aligned} x = 4 \bmod 73 &\Leftrightarrow x = 4,\ 4 + 73,\ 4 + 2 * 73,\ 4 + 3 * 73,\ 4 + 4 * 73 \bmod 365 \\ &\Leftrightarrow x = 4,\ 77,\ 150,\ 223,\ 296 \bmod 365. \end{aligned}$$

Exercice 2

1. $x = y \bmod 2$ équivaut à : il existe $q \in \mathbb{Z}$ tel que $x = y + 2q$. Alors,

$$x^2 = (y + 2q)^2 = y^2 + 4q + 4q^2 = y^2 + 4(q + q^2) = y^2 \bmod 4.$$

2. Comme $x = 0$ ou $1 \bmod 2$, d'après la question précédente, $x^2 = 0^2$ ou $1^2 \bmod 4$, soit $x^2 = 0$ ou $1 \bmod 4$.

1. Soit x et y deux entiers ; d'après la question précédente, $x^2 = 0$ ou $1 \bmod 4$ et $y^2 = 0$ ou $1 \bmod 4$. Donc les possibilités pour $x^2+y^2 \bmod 4$ sont : $0+0, 0+1, 1+0, 1+1 \bmod 4$ soit $0, 1, 2 \bmod 4$ donc on ne trouve pas $3 \bmod 4$.
2. On procède comme à la question 1 : si $x = y + 2^k q$, alors

$$x^2 = (y + 2^k q)^2 = y^2 + 2.2^k q + (2^k q)^2 = y^2 + 2^{k+1} q + 2^{2k} q^2.$$

   On obtient $x^2 = y^2 + 2^{k+1}(q + 2^{k-1} q^2) = y^2 \bmod 2^{k+1}$.
3. On applique le résultat précédent à $k = 2 : x = 0, 1, 2, 3 \bmod 4$ donc $x^2 = 0^2, 1^2, 2^2, 3^2 \bmod 8$ soit $x^2 = 0, 1, 4 \bmod 8$.
4. On vient de démontrer qu'un carré modulo 8 vaut $0, 1, 4$; on calcule toutes les possibilités pour $x^2 + y^2 + z^2 \bmod 8$ à l'ordre près :

$$\begin{aligned} x^2 + y^2 + z^2 = \quad & 0+0+0 = 0 \bmod 8 \\ & 0+0+1 = 0 \bmod 8 \\ & 0+0+4 = 4 \bmod 8 \\ & 0+1+1 = 2 \bmod 8 \\ & 0+1+4 = 5 \bmod 8 \\ & 0+4+4 = 0 \bmod 8 \\ & 1+1+1 = 3 \bmod 8 \\ & 1+1+4 = 6 \bmod 8 \\ & 1+4+4 = 1 \bmod 8 \\ & 4+4+4 = 4 \bmod 8 \end{aligned}$$

   On trouve toutes les valeurs possibles modulo 8 sauf 7.

Exercice 3

1. On trouve $1, 3, 2, 6, 4, 5, 1, 3 \bmod 7$. Il faut montrer que $10^{k+6} = 10^k \bmod 7$ pour tout $k \geq 0$. Mais on a vu que $10^6 = 1 \bmod 7$ donc $10^{k+6} = 10^k.10^6 = 10^k.1 = 10^k \bmod 7$ et la suite est bien périodique de période 6.
2. Notons $r_0 = 1$, $r_1 = 3$, $r_2 = 2$, $r_3 = 6$, $r_4 = 4$, $r_5 = 5$. On a donc $10^{k+6q} = r_k \bmod 7$ pour tout $k = 0, \ldots, 5$ et $q \geq 0$. Soit n un entier dont les chiffres décimaux sont $a_0, a_1, \ldots, a_s$. On a :

$$\begin{aligned} n &= a_0 + a_1 10 + a_2 10^2 + \cdots + a_s 10^s = \sum_{i=0}^{s} a_i 10^i \\ &= (a_0 r_0 + a_1 r_1 + \cdots + a_5 r_5) + (a_6 r_0 + a_7 r_1 + \cdots + a_{11} r_5) + \ldots \bmod 7 \\ &= \sum_{q \geq 0} \Big(\sum_{k=0}^{5} a_{k+6q} r_k \Big) \bmod 7 \end{aligned}$$

   Autrement dit, n est divisible par 7 si et seulement si le nombre obtenu en faisant la somme des produits de ses chiffres décimaux $a_i, i \geq 0$ par les $r_i, i = 0, \ldots, 5$ reproduits cycliquement est divisible par 7.
3. $n = 8641969$. On calcule $9r_0 + 6r_1 + 9r_2 + r_3 + 4r_4 + 6r_5 + 8r_0 = 105$. On peut même itérer : $5r_0 + r_2 = 7$ donc $7|105$ donc $7|n$.