M1MI2016 : Codes et cryptologie 2012/2013

Corrigé du DS n°2

Exercice 1. Résoudre le système de congruences :

$$\begin{cases} x & \equiv 1 \mod 3 \\ x & \equiv 2 \mod 11 \\ x & \equiv 51 \mod 61 \end{cases}$$

Solution. L'algorithme d'Euclide étendu :

r_k	u_k	v_k	q_k
11	1	0	
3	0	1	3
2	1	-3	1
1	-1	4	2

fournit l'égalité de Bézout $4\times3-1\times11=1$. Le système formé des deux premières équations équivaut donc à la congruence $x \equiv a \mod (3\times11)$ avec $a = 1\times(-1\times11)+2\times(4\times3) = 13$. Le système se réduit donc à :

$$\begin{cases} x & \equiv 13 \mod 33 \\ x & \equiv 51 \mod 61 \end{cases}$$

L'algorithme d'Euclide étendu :

r_k	u_k	v_k	q_k
61	1	0	
33	0	1	1
28	1	-1	1
5	-1	2	5
3	6	-11	1
2	-7	13	1
1	13	-24	1

fournit l'égalité de Bézout $13 \times 61 - 24 \times 33 = 1$. Ce système est donc équivalent à la congruence $x \equiv b \mod (33 \times 61)$ avec $b = 13 \times (13 \times 61) + 51 \times (-24 \times 33) = -30083$. Ainsi, le système équivaut à la congruence :

$$x \equiv 112 \mod 2013$$

(en réduisant b modulo $33 \times 61 = 2013$).

Exercice 2. Montrer que pour tout $n \in \mathbb{Z}$, on a $n^7 \equiv n \mod 42$.

Solution. On a $42 = 2 \times 3 \times 7$. Soit $n \in \mathbb{Z}$. D'après le petit théorème de Fermat appliqué avec le nombre premier 2, on a $n^2 \equiv n \mod 2$. On a donc $n^7 = (n^2)^3 \times n \equiv n^4 \mod 2$ donc $n^7 \equiv n^2 \mod 2$ *ie* $n^7 \equiv n \mod 2$. De même on a $n^3 \equiv n \mod 3$, donc $n^7 = (n^3)^2 \times n \equiv n^3 \mod 3$ *ie* $n^7 \equiv n \mod 3$. Enfin, on a aussi $n^7 \equiv n \mod 7$, de sorte que $2 \times 3 \times 7 \mid n^7 - n$, soit encore $n^7 \equiv n \mod 42$.

Exercice 3. On pose

$$f\colon \mathbb{Z}/256\mathbb{Z} \to \mathbb{Z}/256\mathbb{Z}$$
$$x \mapsto 137x + 187$$

et pour $n \in \mathbb{N}_{>0}$, on note $f^{(n)}$ la fonction f itérée n-fois, c'est-à-dire $\underbrace{f \circ f \circ \cdots \circ f \circ f}_{n \text{ fois}}$.

(1) Calculer $f^{(2)}$.

(2) Montrer par récurrence sur $k \in \mathbb{N}$ qu'il existe des suites $(a_k)_{k\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{Z}/256\mathbb{Z}$ telles que :

$$f^{(2^k)}(x) = a_k x + b_k$$

pour tout $x \in \mathbb{Z}/256\mathbb{Z}$ (on précisera la valeur de a_{k+1} en fonction de a_k, et celle de b_{k+1} en fonction de a_k et de b_k).

(3) Calculer les valeurs de a_k et de b_k pour $0 \leq k \leq 8$ (il est conseillé de présenter le résultat sous la forme d'un tableau). En déduire que pour tout $x \in \mathbb{Z}/256\mathbb{Z}$, on a $f^{(256)}(x) = x$.

(4) On considère le générateur linéaire congruentiel dans $\mathbb{Z}/256\mathbb{Z}$ donné par la récurrence linéaire :

$$x_{n+1} = f(x_n) = 137x_n + 187$$

Montrer que toutes les suites engendrées par ce générateur sont de période 256, quelle que soit leur initialisation.

(5) Montrer que l'application $f^{(2^7)}$ n'a pas de point fixe (*ie* d'élément $x \in \mathbb{Z}/256\mathbb{Z}$ tel que $f^{(2^7)}(x) = x$). En déduire que la plus petite période de $(x_n)_{n\in\mathbb{N}}$ vaut 256 (on pourra d'abord montrer qu'elle divise 256).

Solution. (1) On a $f^{(2)}(x) = f(137x+187) = 137(137x+187)+187 = 137^2x+(137+1)\times 187$, soit :

$$f^{(2)}(x) = 81x + 206$$

(en utilisant $137^2 \equiv 81 \mod 256$ et $138 \times 187 \equiv 206 \mod 256$).

(2) On a bien sûr $f(x) = a_0x + b_0$ avec $a_0 = 137$ et $b_0 = 187$, ce qui prouve l'énoncé pour $k = 0$. Supposons maintenant que $(\forall x \in \mathbb{Z}/256\mathbb{Z})\ f^{(2^k)}(x) = a_kx + b_k$. Pour $x \in \mathbb{Z}/256\mathbb{Z}$, on a :

$$\begin{aligned} f^{(2^{k+1})}(x) &= f^{(2^k)}\Big(f^{(2^k)}(x)\Big) \\ &= a_k f^{(2^k)}(x) + b_k \\ &= a_k(a_kx + b_k) + b_k \\ &= a_k^2x + (a_k + 1)b_k \end{aligned}$$

de sorte que $f^{(2^{k+1})}(x) = a_{k+1}x + b_{k+1}$ avec :

$$a_{k+1} = a_k^2 \qquad b_{k+1} = (a_k + 1)b_k$$

ce qui achève la récurrence.

(3) En utilisant les formules de la question précédente, on obtient :

k	0	1	2	3	4	5	6	7	8
a_k	137	81	161	65	129	1	1	1	1
b_k	187	206	252	120	240	224	192	128	0

En particulier, on a $f^{(2^8)}(x) = x$ pour tout $x \in \mathbb{Z}/256\mathbb{Z}$, de sorte que $f^{(2^8)} = \mathrm{Id}_{\mathbb{Z}/256\mathbb{Z}}$.

(4) D'après la question précédente, on a $x_{n+256} = f^{(2^8)}(x_n) = x_n$ pour tout $n \in \mathbb{N}$: la suite $(x_n)_{n\in\mathbb{N}}$ est périodique de période 256 (indépendamment de x_0).

(5) D'après la question (3), on a $f^{(2^7)}(x) = x + 128$ pour tout $x \in \mathbb{Z}/256\mathbb{Z}$: comme $128 \neq 0$ dans $\mathbb{Z}/256\mathbb{Z}$, l'équation $f^{(2^7)}(x) = x$ n'a pas de solution, *ie* $f^{(2^7)}$ n'a pas de point fixe.

On sait que $(x_n)_{n\in\mathbb{N}}$ est périodique : soit $T \in \mathbb{N}_{>0}$ la plus petite période. D'après la question précédente, on a $T \leq 2^8$: soit $2^8 = qT + r$ la division euclidienne de 2^8 par T. Pour tout $n \in \mathbb{N}$, on a $x_n = x_{n+2^8} = x_{n+r+qT} = x_{n+r}$ par T-périodicité : la suite $(x_n)_{n\in\mathbb{N}}$ est aussi r-périodique. Comme $r < T$, on a nécessairement $r = 0$ par minimalité de T, de sorte que $T \mid 2^8$. On a donc $T = 2^k$ avec $k \leq 8$. Si on avait $k < 8$, on aurait $T \mid 2^7$, donc $f^{(2^7)}(x_n) = x_{n+2^7} = x_n$, et x_n serait un point fixe de $f^{(2^7)}$ pour tout $n \in \mathbb{N}$. C'est impossible en vertu de ce qu'on a vu plus haut : on a nécessairement $T = 2^8 = 256$.

Exercice 4. Alice et Bob communiquent en utilisant le protocole RSA. La clé publique de Bob est $N = 209$ et $e = 7$.
(1) Alice veut transmettre le message $m = 5$ à Bob : quel message M va-t-il recevoir ?
(2) Quelle est la clé secrète de Bob ?
(3) Bob reçoit $M = 2$: quel est le message m qu'Alice lui a envoyé ?

Solution. (1) M est le reste de $5^7 = 78125$ modulo 209, *ie* $M = 168$.

(2) On a $N = 11 \times 19$, de sorte que $\varphi(209) = (11-1)(19-1) = 180$. L'algorithme d'Euclide étendu :

r_k	u_k	v_k	q_k
180	1	0	
7	0	1	25
5	1	-25	1
2	-1	26	2
1	3	-77	2

fournit l'égalité de Bézout $3 \times 180 - 77 \times 7 = 1$. Comme $-77 \equiv 103 \mod 180$, la clé secrète de Bob est $d = 103$.

(3) m est le reste de 2^{103} modulo 209. On a $2^7 = 128 < 209 < 2^8 = 256$: écrivons $103 = 8 \times 12 + 7$. On a $2^8 \equiv 47 \mod 209$, donc :

k	1	2	4	12
2^{8k}	47	119	158	64

Ainsi, $2^{103} \equiv 64 \times 128 \mod 209$, soit $m = 41$.

On peut aussi utiliser le théorème chinois pour calculer m. On a $2^{10} \equiv 1 \mod 11$ donc $2^{103} \equiv 2^3 \mod 11$ *ie* $m \equiv 8 \mod 11$, et $2^{18} \equiv 1 \mod 19$ donc $2^{103} \equiv 2^{13} \mod 19$ *ie* $m \equiv 3 \mod 19$: on vérifie sans peine que $m = 41$ en utilisant l'égalité de Bézout $7 \times 11 - 4 \times 19 = 1$.