M1MI2016 Codes et Cryptologie

Corrigé du DS n° 1.

$\boxed{1}$ Pour décider si 583 est inversible modulo 679, et le cas échéant calculer son inverse, on applique l'algorithme d'Euclide étendu.

r_k	u_k	v_k	q_k	
679	1	0		
583	0	1	1	$(679 = 583 * 1 + 96)$
96	1	-1	6	$(583 = 96 * 6 + 7)$
7	-6	7	13	$(96 = 7 * 13 + 5)$
5	79	-92	1	$(7 = 5 * 1 + 2)$
2	-85	99	2	$(5 = 2 * 2 + 1)$
1	249	-290		

Le pgcd de 679 et 583 est égal à 1 donc 583 est inversible modulo 679 et on a la relation de Bezout : $679 * 249 - 583 * 290 = 1$ qui montre que $583^{-1} = -290 \mod 679$.

$\boxed{2}$ On pouvait remarquer que $2^m - 1$ est impair, alors que 2^n a pour seul diviseur premier 2, donc que ces deux nombres sont premiers entre eux. Cela montre que 2^n est inversible modulo $2^m - 1$ mais ne suffit pas à calculer son inverse.

Pour cela, il fallait remarquer que

$$2^n * 2^{m-n} = 2^m = 1 + (2^m - 1) = 1 \mod (2^m - 1)$$

ce qui prouve à la fois que 2^n est inversible modulo $2^m - 1$, et son inverse est 2^{m-n}.

Autre solution : on pouvait tenter l'algorithme d'Euclide sur $2^m - 1$ et 2^n, donc effectuer la division euclidienne de $2^m - 1$ par 2^n. Elle est donnée par : $2^m - 1 = 2^n * 2^{m-n} - 1$, le reste est donc -1. Cette égalité donne immédiatement que $2^n * 2^{m-n} = 1 \mod (2^m - 1)$ soit que 2^n est inversible modulo $2^m - 1$, d'inverse 2^{m-n}.

$\boxed{3}$

$$\begin{aligned} 2x + 3 = 5 \mod 11 &\Longleftrightarrow 2x = 2 \mod 11 \\ &\Longleftrightarrow x = 1 \mod 11 \quad \text{car 2 est inversible modulo 11.} \end{aligned}$$

L'ensemble des solutions est $S = \{1 \mod 11\}$.

$$3x + 7 = 5 \mod 9 \Longleftrightarrow 3x = -2 \mod 9.$$

Comme $\mathrm{pgcd}(3, 9) = 3 \neq 1$, 3 n'est pas inversible modulo 9. Comme 3 ne divise pas -2, il n'y a pas de solutions : $S = \emptyset$.

$$\begin{aligned}6x-4=8 \mod 9 &\iff 6x=12 \mod 9\\ &\iff 2x=4 \mod 3 = 1 \mod 3\\ &\iff x=2 \mod 3 \quad \text{car 2 est inversible modulo 3 et } 2^{-1}=2 \mod 3\\ &\iff x=2,5,8 \mod 9.\end{aligned}$$

Dans ce cas on a trois solutions : $S=\{2,5,8 \mod 9\}$.

$\boxed{4}$

1.

a	0	1	2	3	4	5	6	mod 7
a^2	0	1	4	2	2	4	1	mod 7
a^6	0	1	1	1	1	1	1	mod 7

2. Si x, y éléments de $\mathbb{Z}$ sont tels que $x^2-2y^6=17$, alors $x^2-2y^6=17=3 \mod 7$. D'après le tableau, $y^6=0 \mod 7$ ou $y^6=1 \mod 7$. Donc,

$$\begin{aligned}x^2 = 2y^6+3 &= 2*0+3=3 \mod 7\\ \text{ou bien } &= 2*1+3=5 \mod 7.\end{aligned}$$

3. Supposons par l'absurde que x, y sont des éléments de $\mathbb{Z}$ tels que $x^2-2y^6=17$. D'après la question précédente, $x^2=3$ ou $5 \mod 7$. Mais, d'après le tableau de la question 1., on a $x^2=0,1,2,4 \mod 7$ mais pas $3,5 \mod 7$ on a donc aboutit à une contradiction. Donc il n'existe pas d'entiers x, y tels que $x^2-2y^6=17$.