# M1MI2016 Codes et Cryptologie

## DS n° 1.

**7 Mars 2012, durée 1h20**

Documents interdits, calculatrices autorisées

**Le sujet n'est pas long, et est proche de ce qui a été fait en TD. En contrepartie on attend de vous une rédaction soignée.**

1 L'entier 583 est-il inversible modulo 679 ? Si oui, calculez son inverse.

2 Soit $n \leq m$ deux entiers positifs. Montrez que $2^n$ est inversible modulo $2^m - 1$ et calculez son inverse.

3 Résoudre les équations suivantes :

$$\begin{aligned} 2x + 3 &= 5 \mod 11 \\ 3x + 7 &= 5 \mod 9 \\ 6x - 4 &= 8 \mod 9 \end{aligned}$$

4 Le but de cet exercice est de montrer qu'il n'existe pas d'entiers $x, y$ tels que $x^2 - 2y^6 = 17$.

1. Complétez le tableau suivant, dont les entrées sont des éléments de $\mathbb{Z}/7\mathbb{Z}$ :

| $a$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | mod 7 |
|---|---|---|---|---|---|---|---|---|
| $a^2$ | | | | | | | | |
| $a^6$ | | | | | | | | |

2. Déduire de la question précédente que, si $x, y$ éléments de $\mathbb{Z}$ sont tels que $x^2 - 2y^6 = 17$, alors $x^2 = 3 \mod 7$, ou bien $x^2 = 5 \mod 7$.
3. En utilisant à nouveau le tableau de la question 1., montrez qu'il n'existe pas d'entiers $x, y \in \mathbb{Z}$ tels que $x^2 - 2y^6 = 17$.