Cryptologie
MHT203

Feuille d'exercices 7

Petit théorème de Fermat

Exercice 1.
On sait d'après le petit théorème de Fermat, que si p est un nombre premier, pour tout a premier avec p on a : $a^{p-1} = 1 \bmod p$. On va montrer que la réciproque est fausse, c'est-à-dire, qu'il existe des entiers n qui ne sont pas premiers et pour lesquels on a aussi pour tout a premier avec n l'égalité $a^{p-1} = 1 \bmod n$ est vérifiée. Ce sont des nombres pseudo-premiers ou encore les nombres de Carmichael.

1. Décomposer 561 en produit de facteurs premiers.

2. Montrer que si a est premier avec 561 alors :

$$\begin{aligned} a^{560} &\equiv 1 \bmod 3 \\ a^{560} &\equiv 1 \bmod 11 \\ a^{560} &\equiv 1 \bmod 17 \end{aligned}$$

Indication : penser à utiliser le théorème de Fermat.

3. Montrer que pour tout a premier avec 561 on a $a^{560} = 1 \bmod 561$.

(561 est le plus petit nombre de Carmichael, mais il en existe en fait une infinité.)

Exercice 2.
Déterminer l'ordre des éléments de $(\mathbb{Z}/7\mathbb{Z})^*$ et vérifier le théorème de Fermat.

Exercice 3.

1. Calculer modulo 100 : $6^2, 6^{2^2}, 6^{2^3}, 6^{2^4}, 6^{2^5}, 6^{2^6}$. On pourra utiliser : $6^{2^{k+1}} = \left(6^{2^k}\right)^2$.

2. Calculer modulo 100 : 6^{73}. On pourra remarquer que $73 = 1 + 2^3 + 2^6$ et utiliser la question précédente.

Exercice 4.

1. Ecrire 340 en base 2.

2. En utilisant la méthode de l'exponentiation rapide, calculer modulo 340 3^{2^k} pour $k = 1, 2, 3, 4, 5, 67, 8$. En déduire que $3^{340} \equiv 56 \bmod 341$. Que peut-on dire de 341 ?

Exercice 5.

On suppose que l'on veut calculer x^k avec $x \in \mathbb{Z}$ et $k \in \mathbb{N}$. On va appliquer la méthode suivante :

1. Ecrire l'entier k en base 2

$$k = \sum_{i=0}^{q} a_i 2^i = \overline{a_q a_{q-1} \dots a_1 a_0}$$

avec $a_q = 1$ et $a_i \in \{0, 1\}$.

2. Dans l'écriture précédente on remplace 1 par CM et 0 par C. On obtient une suite finie de C et de M qui commence par CM (puisque $a_q = 1$).

3. On fait : $z \leftarrow 1$; puis on lit la suite de gauche à droite et si on lit C (carré) on fait $z \leftarrow z^2$ et si on lit M (multiplier) on fait $z \leftarrow z.x$.

4. Vérifier que l'on obtient à la fin de l'algorithme x^k.

5. Calculer aver cette méthode $54^{13} \bmod 59$ et $563^{1234} \bmod 612$.