Université Bordeaux 1 — **MHT203 – Cryptologie**
Mathématiques — Année 2012–2013

FEUILLE D'EXERCICES n° 7
Petit théorème de Fermat

Exercice 1 – Si p est premier, on a $a^{p-1} = 1 \bmod p$ pour tout a premier avec p. La réciproque est fausse : il existe des entiers n non premiers, pour lesquels l'égalité $a^{n-1} = 1 \bmod n$ est vérifiée pour tout a premier avec n ; ce sont les *nombres de Carmichael* (il en existe une infinité).

1) Décomposer 561 en produit de facteurs premiers.

2) Montrer que, si a est premier avec 561, alors :

$$a^{560} \equiv 1 \bmod 3, \quad a^{560} \equiv 1 \bmod 11, \quad a^{560} \equiv 1 \bmod 17.$$

[*Utiliser le théorème de Fermat !*]

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

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}. [*Remarquer que* $73 = 1 + 2^3 + 2^6$.]

Exercice 4 –

1) Ecrire 340 en base 2.

2) En utilisant la méthode de l'exponentiation rapide, calculer modulo 340 3^{2^k} pour $k = 1, \ldots, 8$. En déduire que $3^{340} \equiv 56 \bmod 341$. L'entier 341 est-il premier ?

Exercice 5 – On veut calculer x^k avec $x \in \mathbb{Z}$ et $k \in \mathbb{Z}_{>0}$.

1) On applique la méthode suivante :

a) Ecrire l'entier k en base 2

$$k = \sum_{0 \leqslant i \leqslant q} a_i 2^i = \overline{a_q a_{q-1} \ldots a_1 a_0}, \quad \text{avec } a_q = 1 \text{ et } a_i \in \{0, 1\}.$$

b) Dans cette écriture, remplacer 1 par CM et 0 par C. On obtient une suite de C et de M, qui commence par CM puisque $a_q = 1$.

c) On initialise $z \leftarrow 1$; puis on lit la suite de gauche à droite : si on lit C (resp. M) on remplace $z \leftarrow z^2$ (resp. $z \leftarrow z \times x$).

2) Vérifier que l'on obtient $z = x^k$ à la fin de l'algorithme

3) Calculer avec cette méthode $54^{13} \bmod 59$ et $563^{1234} \bmod 612$.