Cryptologie
MHT203

Feuille d'exercices 2
Congruences

Exercice 1.
1) Faire la table d'addition et de multiplication dans $\mathbb{Z}/6\mathbb{Z}$ puis dans $\mathbb{Z}/7\mathbb{Z}$.
2) Donner la liste des éléments de $\mathbb{Z}/6\mathbb{Z}$ (puis dans $\mathbb{Z}/7\mathbb{Z}$) tels que si on multiplie deux éléments de cette liste on obtienne 1 modulo 6 (respectivement 1 modulo 7).
3 Donner la liste des éléments de $\mathbb{Z}/6\mathbb{Z}$ tels que si on multiplie deux éléments de cette liste on obtienne 0 modulo 6.

Exercice 2.
1. Calculer $35 \pmod{11}$. Calculer $2^i \pmod{11}$ pour $i = 2, \ldots, 5$ et $i = 10$.
2. En déduire $35^{57} \pmod{11}$.
3. Appliquer la méthode précédente pour calculer $9518^{18} \pmod{5}$.

Exercice 3.
1) Que signifie la phrase "n est congru à 1 modulo 3" ?
2) Traduire à l'aide d'une congruence "n est divisible par 3".
3) Pour chacun des nombres suivants, donner l'entier positif le plus petit auquel il est congru modulo 3 : 1, 10, 100, 1000, 10^k où k est un entier positif.
4) A l'aide de la question précédente, déterminer le plus petit entier positif auquel est congru 4520 modulo 3.
5) Soit $n = a_k a_{k-1} \ldots a_0 = a_k.10^k + a_{k-1}.10^{k-1} + \cdots + a_0.10^0$ un entier. Montrer que $n = a_k + a_{k-1} + \cdots + a_0 \mod 3$. En déduire qu'un entier est divisible par trois si et seulement si la somme de ces chiffres est divisible par trois.

Exercice 4. Le but de cet exercice est de montrer que, pour tout entier naturel n, le nombre $A = n(n^2 - 1)$ est égal à 0 modulo 6.
1) Dans chacun des cas suivants, calculer A et déterminer A modulo 6 : $n = 5$; $n = 16$; $n = 32$.
2) En donnant dans un tableau les différentes valeurs de n modulo 6, de $n - 1$ modulo 6 et de $n + 1$ modulo 6, démontrer le résultat.

Exercice 5.
1) Ecrire les tables d'addition et de multiplication dans $\mathbb{Z}/4\mathbb{Z}$.
2) En utilisant ces tables résoudre dans $\mathbb{Z}/4\mathbb{Z}$ les équations :

$$3x + 2 = 1; \quad 3x = 2; \quad 2x = 1; \quad 2x = 2.$$

3) Soient a, b et c trois éléments de $\mathbb{Z}/4\mathbb{Z}$. S'il existe a' dans $\mathbb{Z}/4\mathbb{Z}$ tel que $aa' = 1 \mod 4$ que peut-on dire de l'équation $ax + b = c$?