Université Bordeaux 1
Mathématiques

MHT203 – Cryptologie
Année 2012–2013

FEUILLE D'EXERCICES n° 2

Congruences

Exercice 1 –

1) Écrire la table d'addition et de multiplication dans $\mathbb{Z}/6\mathbb{Z}$; donner la liste des $x \in \mathbb{Z}/6\mathbb{Z}$ tels qu'il existe $y \in \mathbb{Z}/6\mathbb{Z}$ tel que $xy = 1$.

2) Donner la liste des $x \in \mathbb{Z}/6\mathbb{Z}$ tels qu'il existe $y \in \mathbb{Z}/6\mathbb{Z}$, $y \neq 0$, tel que $xy = 0$.

3) Mêmes questions dans $\mathbb{Z}/7\mathbb{Z}$.

Exercice 2 –

1) Déterminer 35 modulo 11 ; montrer que $2^5 \equiv 10 \pmod{11}$ et en déduire que $35^{57} - 7$ est un multiple de 11.

2) En procédant de manière analogue, montrer que $9518^{42} \equiv 4 \pmod 5$.

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) À l'aide de la question précédente, déterminer le plus petit entier positif auquel est congru 4520 modulo 3.

5) Soit $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_0 \cdot 10^0$ un entier. Montrer que $n \equiv a_k + a_{k-1} + \cdots + a_0 \pmod 3$. En déduire qu'un entier est divisible par trois si et seulement si la somme de ces chiffres est divisible par trois.

6) Trouver des critères analogue de divisibilité par 9, puis par 11.

Exercice 4 – Le but de cet exercice est de montrer que, pour tout $n \in \mathbb{N}$, le nombre $A = n(n^2 - 1)$ est égal à 0 modulo 6.

1) Calculer A, puis A modulo 6 dans chacun des cas suivants : $n = 5$; $n = 16$; $n = 32$.

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) Écrire les tables d'addition et de multiplication dans $\mathbb{Z}/4\mathbb{Z}$, puis résoudre dans $\mathbb{Z}/4\mathbb{Z}$ les équations

$$3x + 2 = 1; \quad 2x = 0; \quad 2x = 1; \quad 2x = 2; \quad 2x = 3.$$

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

Exercice 6 – Résoudre l'équation $18x - 14y = 22$ où x et y sont des entiers.