Licence première année 2011-2012

M1MI2016 Codes et Cryptologie : feuille d'exercices 2

– Exercice 1.

1. Écrire les tables d'addition et de multiplication dans $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$.
2. Dans les deux cas, donner la liste des éléments inversibles ainsi que leurs inverses.
3. Résoudre (trouver *l'ensemble* des solutions) les équations

$$5x - 3 = 1 \bmod 7$$
$$3x + 7 = 0 \bmod 7$$
$$3x + 4 = 1 \bmod 8$$
$$2x + 5 = 1 \bmod 8$$
$$4x + 3 = 1 \bmod 8.$$

– Exercice 2.

1. À quoi reconnaissez-vous qu'un entier écrit en base 10 est divisible par 2 ? Par 5 ? Par 3 ? Par 9 ? Expliquez le résultat en termes de congruences modulo 2,5,3,9.
2. Montrer qu'un entier dont l'écriture en base 10 est $a_{m-1} \dots a_1 a_0$ est divisible par 11 si et seulement si $a_0 - a_1 + a_2 + \cdots + (-1)^{m-1} a_{m-1} = 0 \bmod 11$.
3. Sans utiliser de calculatrice et sans poser de division, établir une règle de divisibilité par 101 et montrer que 478775514327 est divisible par 101.
4. Trouver un critère permettant de savoir simplement si un entier dont l'écriture en base 2 est $a_{m-1} \dots a_1 a_0$ est divisible par 7. L'entier 101101010110111 est-il divisible par 7 ?

– Exercice 3. Montrer que pour tout entier n, $n(n^2 - 1)$ est divisible par 6 : ramenez-vous à l'examen d'un nombre fini d'entiers.

– Exercice 4. Trouver les inverses de 37 modulo 139, de 88 modulo 103, de 24 modulo 107.

– Exercice 5. Résoudre dans $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ le système d'équations :

$$2x + y = 3$$
$$5x - 4y = 2.$$

– Exercice 6.

1. Quels sont les éléments de $\mathbb{Z}/13\mathbb{Z}$ qui sont des carrés (les éléments x qui s'écrivent $x = a^2$) ? Même question pour $\mathbb{Z}/15\mathbb{Z}$.
2. Utiliser le lemme de Gauss pour montrer que si $a^2 = b^2 \bmod p$ où p est premier, alors dans $\mathbb{Z}/p\mathbb{Z}$ on a $b = a$ ou $b = -a$.
3. Soit $n = 11021$. Quel est le plus petit entier a tel que que $a^2 > n$?
4. Calculer $a^2 \bmod n$ et en déduire une égalité du type : $a^2 = b^2 \bmod n$.
5. Appliquer le point 2. pour en déduire que n n'est pas premier.
6. Pousser le même raisonnement pour exhiber un entier y dont le pgcd avec n ne peut pas être égal à 1. Calculer le pgcd de n et de y et en déduire la décomposition de n en facteurs premiers.
7. Appliquer la même méthode (qui est due à Fermat) pour trouver les facteurs premiers de 67591.

– Exercice 7. On réunit cinq équipes de basket de cinq joueurs chacune. Les joueurs de chaque équipe portent des maillots numérotés de 1 à 5. Pour la cérémonie d'ouverture du tournoi, on trouve que ça ferait joli de disposer les 25 joueurs en carré 5×5, de telle sorte que dans chaque ligne ainsi que dans chaque colonne on voit 5 joueurs n'appartenant qu'à des équipes différentes et ne portant que des numéros différents.

Montrer que si un joueur est déterminé par son couple (équipe, numéro), une solution au problème consiste à mettre en position (i, j) du tableau carré le joueur de l'équipe $i+j \bmod 5$ et au numéro $i+2j \bmod 5$. Montrer que la solution marche encore pour des équipes de p joueurs, quand p est premier.

– Exercice 8.

1. Écrire les premières lignes du triangle de Pascal, et constater que tous les coefficients de la p-ième ligne (121 est la deuxième ligne) qui ne sont pas '1' sont divisibles par p.
2. Le démontrer. On se rappellera que les termes de la p-ième ligne sont les coefficients binomiaux $\binom{p}{i}$ et commencera par montrer que si $k < p$ alors p ne divise pas $k!$.