Licence STS — mention mathématiques *Année 2005/2006*

A2. NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES. PERMUTATIONS

Feuille de travaux dirigés n° 5 : *Congruences*

EXERCICE 1

Le code ISBN a été inventé dans les années 60 pour faciliter le travail de catalogage des livres dans les bibliothèques. Il se compose de 10 chiffres décimaux séparés par des espaces ou des tirets, dont le dernier peut aussi être le symbole X représentant la valeur 10. Le premier représente la langue (0 pour l'anglais, 2 pour le français, 3 pour l'allemand...), le bloc suivant l'éditeur (Springer-Verlag en Allemagne : 540, aux États-Unis : 387, Cassini : 84225, Dargaux : 205, etc.), le suivant le numéro du livre chez l'éditeur — il reste d'autant peu de place que l'éditeur a un gros numéro — et le dernier est un code permettant de s'assurer (au moins partiellement) de l'intégrité du code. Si les 10 chiffres sont $a_1, \dots, a_{10}$, la condition qu'ils doivent vérifier s'écrit

$$\sum_{i=1}^{10} i\,a_i \equiv 0 \pmod{11}.$$

1 Vérifier que 2-205-00694-0 (*Astérix en Corse*) et 0-387-54894-7 (*Introduction to Coding Theory* de J. H. van Lint) sont des codes ISBN valides.

2 Vérifier que 2-84225-007-1 n'est pas un ISBN valide. Peut-on le corriger ?

3 Montrer que l'on peut détecter un chiffre inexact, ou l'interversion de deux chiffres dans un ISBN (en supposant qu'il n'y ait qu'une seule erreur de ce type).

EXERCICE 2

Le code de sécurité sociale est formé de 13 chiffres décimaux suivi d'une clef de deux chiffres. Si N est l'entier de 13 chiffres et c la clef, la contrainte de vérification est la relation

$$N + c \equiv 0 \pmod{97}.$$

1 Quelle est la clef d'un individu dont le numéro de sécurité sociale serait 1-71-04-78-646-378 ?

2 Un numéro de sécurité sociale est 2-xx-07-35-231-584, clé 19, mais les caractères xx sont illisibles. Pouvez-vous retrouver l'année de naissance de la personne en question ? (Solution : 1943)

3 Montrer que la clef de contrôle détecte une erreur sur un chiffre, ainsi que l'interversion de deux chiffres consécutifs.

4 Montrer que 97 est un nombre premier et que $n = 96$ est le plus petit entier > 0 tel que $10^n \equiv 1 \pmod{97}$.

5 Montrer plus généralement que la clef de contrôle détecte l'interversion de deux chiffres quelconques.

EXERCICE 3

Soit φ l'application de $\{0, \dots, 9\}$ dans lui-même définie par $\varphi(x) = 2x$ si $x \leqslant 4$ et $\varphi(x) = 1 + 2(x-5)$ si $x \geqslant 5$. Un numéro de carte bancaire est un nombre décimal de la forme $a_n a_{n-1} \dots a_1 a_0$, où les chiffres décimaux satisfont à la règle (dite de Luhn) :

$$a_0 + \varphi(a_1) + a_2 + \varphi(a_3) + \cdots \equiv 0 \pmod{10}.$$

1 Montrer que cela permet de détecter la présence d'un chiffre décimal erroné.

2 Montrer que cela permet de détecter une permutation de deux chiffres consécutifs, à l'exception de la permutation $09 \to 90$.

Avant l'introduction de l'Euro, les billets de banque allemands utilisaient paraît-il un code obtenu par l'adjonction d'un chiffre décimal à un nombre décimal de 9 chiffres qui détectait une erreur ou l'interversion de deux chiffres consécutifs.

EXERCICE 4

1 Montrer que pour tout entier n, $n(n^4-1)$ est divisible par 15.

2 Montrer que pour tout entier n, $n^2(n^4-1)$ est divisible par 60. Peut-on faire mieux ?

3 Montrer que pour tout entier n, $n(n^6-1)$ est divisible par 42. Peut-on faire mieux ?

EXERCICE 5

Pour chaque valeur de l'entier n, $2 \leqslant n \leqslant 20$, calculer $\varphi(n)$ en dénombrant les entiers de $\{1,\ldots,n\}$ qui sont premiers avec n.

EXERCICE 6

1 Calculer $\varphi(n)$ si n est une puissance d'un nombre premier p.

2 En utilisant le théorème chinois, démontrer que $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont des entiers premiers entre eux.

3 En déduire $\varphi(n)$ en fonction de la décomposition en facteurs premiers de n.

EXERCICE 7

Soit n un entier qui est le produit de deux nombres premiers distincts. Montrer que pour tout $x \in \mathbf{Z}$, on a $x^{\varphi(n)+1} \equiv x \pmod{n}$.

EXERCICE 8

Soit n un entier $\geqslant 2$; si $0 \leqslant k \leqslant n-1$, on note $c_k = \exp(2ik\pi/n)$.

1 Montrer que $\{c_0,\ldots,c_n\}$ est l'ensemble des racines complexes du polynôme X^n-1.

2 Soit $c \in \mathbf{C}^*$; on suppose que $c^n = 1$. Soit d le plus petit entier >0 tel que $c^d = 1$. (On dit que c est d'ordre d.) Montrer que n est multiple de d.

3 On suppose que n est le plus petit entier >0 tel que $c^n = 1$. Montrer qu'il existe un unique entier $k \in \{0,\ldots,n\}$ tel que $\operatorname{pgcd}(k,n) = 1$ et tel que que $c = c_k$. Combien y a-t-il de tels nombres complexes c ?

4 Plus généralement, si d divise n, combien y a-t-il d'éléments $c \in \mathbf{C}^*$ qui sont d'ordre d ?

5 Montrer que $\sum_{d \mid n} \varphi(d) = n$, où la somme est prise sur l'ensemble des diviseurs >0 de n.

1. Théorème chinois

EXERCICE 1

Quel est le plus petit entier plus grand que $10\,000$ qui divisé par 5, 12 et 17 ait pour reste 3 ?

EXERCICE 2

Trouver tous les entiers compris entre 100 et 1000 qui divisés par 21 aient pour reste 8 et par 17 pour reste 5.

EXERCICE 3

Sachant que le 1er janvier 1901 était un mardi, combien de vendredi 13 y a-t-il eu au XXe siècle ? Dans le calendrier grégorien, calculer les fréquences des lundi 13, mardi 13, etc.

EXERCICE 4

Une vieille fermière s'en allant marché voit ses œufs écrasés par un cheval. Le cavalier voulant la rembourser lui demande combien d'œufs elle avait. Tout ce dont elle se souvient est qu'en les rangeant par 2, il en restait un, et de même en les rangeant par 3, 4, 5 ou 6 ; toutefois, en les rangeant par 7, il n'en restait pas. Combien d'œufs, au moins, avait-elle ? (D'après Lauritzen, repris de Ore)

EXERCICE 5

Sur une ile déserte, cinq hommes et un singe ramassent des noix de coco. La nuit tombée, il s'endorment. Le premier homme se réveille et prend sa part du butin : il divise le tas de noix en cinq parts égales et donne au singe la noix de coco restante, prend sa part et va se recoucher. Le second se réveille, prend un cinquième du tas restant et donne au singe une noix qui restait à part. Et ainsi de suite des cinq hommes. Combien de noix de coco, au moins, avaient été ramassées ? (D'après Lauritzen)

EXERCICE 6

« Une dame ayant rencontré des pauvres, a eu la pensée charitable de leur donner ce qu'elle avait. Pour donner à chacun 9 sous, il lui en manquait 32 ; alors elle leur a donné 7 sous, et il lui en est resté 24. Combien avait-elle et quel est le nombre des pauvres ? » (J. Vinot, *Récréations mathématiques*, années 30).

EXERCICE 7

L'armée de César comptait plus de 1000 hommes, mais moins de 3000. Lorsqu'il voulut la dénombrer par groupes de 11, il n'en resta pas ; par groupes de 9, il en resta 5 ; par groupes de 13, il en resta 8. Combient y avait-il de soldats dans cette armée ? (D'après J. Vinot)

EXERCICE 8

Dix-sept pirates s'emparent d'un lot de pièces d'or toutes identiques. Leur loi exige un partage à égalité : chacun doit recevoir le même nombre de pièces d'or et, s'il y a un reste, celui-ci est attribué au cuisinier de bord. Dans le cas présent, la part du cuisinier serait de trois pièces, mais les pirates se querellent et six d'entre eux sont tués, ce qui porte la part du cuisinier à quatre pièces. Au cours d'une terrible tempête, le bateau fait naufrage et ne survivent que six pirates et le cuisinier. Par bonheur, le butin est sauvé. La part du cuisinier est maintenant de cinq pièces. Que peut espérer gagner le cuisinier lorsqu'il décide d'empoisonner le reste de l'équipage, sachant que c'est la plus petite des solutions possibles ?