Université Paris 7 Année 2008-2009
MI4

Feuille d'exercices n° 3

1. Soit n un entier positif dont l'écriture en base 10 est $a_r a_{r-1} \dots a_0$ ($0 \leq a_k \leq 9$).
   (a) Montrer que $n \equiv \sum_{k=0}^{r} a_k \pmod 9$ et que $n \equiv \sum_{k=0}^{r} (-1)^k a_k \pmod{11}$.
   (b) Écrire un algorithme qui donne le reste de la division de n par 9 (resp. 11), sans faire de division.
2. On considère un nombre de 6 chiffres qui est divisible par 13. On fait passer le premier chiffre à la fin. Montrer que le nouveau nombre est encore divisible par 13.
3. Soit n un entier. Montrer que :
   (a) 29 divise $2^{5n+1} + 3^{n+3}$.
   (b) 17 divise $2^{7n+1} + 3^{2n+1} + 5^{10n+1} + 7^{6n+1}$.
   (c) 18 divise $2^{2n+2} + 24n + 14$.
4. (Une preuve du petit théorème de Fermat...) Soit p un nombre premier, $a \in \mathbb{Z}$ tel que p ne divise pas a, et $\overline{a}$ l'image de a dans $\mathbb{Z}/p\mathbb{Z}$.
   (a) Montrer qu'il existe un élément $\overline{b}$ de $\mathbb{Z}/p\mathbb{Z}$ tel que $\overline{a}\overline{b} = \overline{1}$. En déduire que l'application $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ définie par $f(\overline{x}) = \overline{ax}$ est bijective.
   (b) Montrer que $\prod_{x=1}^{p-1} f(\overline{x}) = \overline{(p-1)!}$.
   (c) Montrer que $a^{p-1} \equiv 1 \pmod p$ et que $a^p \equiv a \pmod p$. Ces congruences sont-elles encore vraies si p divise a ?
5. (...et une autre). Soit p un nombre premier.
   (a) Montrer que pour $1 \leq k \leq p-1$, p divise le coefficient du binôme C_p^k.
   (b) Montrer par récurrence que pour tout entier $n \geq 0$, $n^p \equiv n \pmod p$, puis que cela est aussi vrai pour $n < 0$.
6. Soit n un nombre entier. Montrer que :
   (a) $3n^5 + 5n^3 + 7n$ est divisible par 15.
   (b) $n^5 - n$ est multiple de 30.
   (c) 2730 divise $n^{13} - n$.
7. Déterminer les $x \in \mathbb{Z}$ qui vérifient :
   (a) $7x \equiv 4 \pmod{30}$
   (b) $35x \equiv 15 \pmod{1000}$
   (c) $49x \equiv 5 \pmod{21}$
8. (Théorème de Wilson) Soit p un nombre premier, $p \neq 2$.
   (a) Montrer que $-\overline{1}$ est le seul élément d'ordre 2 du groupe multiplicatif $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$.
   (b) Montrer que $(p-1)! \equiv -1 \pmod p$. Indication : regrouper $\overline{x}$ et $\overline{x}^{-1}$ dans le produit des $\overline{x}$ pour $\overline{x} \in \mathcal{U}(\mathbb{Z}/p\mathbb{Z})$.
   (c) Montrer que si $n > 1$ est un entier qui n'est pas un nombre premier, alors $(n-1)!$ n'est pas congru à -1 modulo n.
9. Déterminer l'ordre de chaque élément des groupes suivants :
   (a) $(\mathbb{Z}/10\mathbb{Z}, +)$
   (b) $(\mathcal{U}(\mathbb{Z}/10\mathbb{Z}), \times)$
   (c) $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, +)$

10. (a) Déterminer les sous-groupes des groupes (a) et (b) de l'exercice 9.

    (b) Soient G_1 et G_2 deux groupes, H_1 et H_2 des sous-groupes de G_1 et G_2 respectivement. Montrer que $H_1 \times H_2$ est un sous-groupe de $G_1 \times G_2$.

    (c) Soient $G_1 = \mathbb{Z}/4\mathbb{Z}$, $G_2 = \mathbb{Z}/6\mathbb{Z}$. Montrer que $G = G_1 \times G_2$ a un sous-groupe qui n'est pas de la forme $H_1 \times H_2$ où $H_1 \subset G_1$ et $H_2 \subset G_2$.

11. (a) Soit $a \in \mathbb{Z}$. Montrer que l'application $\overline{x} \mapsto \overline{ax}$ est un endomorphisme du groupe additif $\mathbb{Z}/10\mathbb{Z}$. (On appelle endomorphisme d'un groupe G un morphisme de groupe de G dans G).

    (b) Soit f un endomorphisme du groupe additif $\mathbb{Z}/10\mathbb{Z}$ et $\overline{a} = f(\overline{1})$. Montrer que pour tout $\overline{x} \in \mathbb{Z}/10\mathbb{Z}$, $f(\overline{x}) = \overline{ax}$.

    (c) Montrer que l'endomorphisme f de la question (b) est bijectif si et seulement si $\overline{a} \in \{\overline{1}, -\overline{1}, \overline{3}, -\overline{3}\}$.

    (d) Montrer que l'ensemble des endomorphismes bijectifs de $\mathbb{Z}/10\mathbb{Z}$ est un groupe isomorphe au groupe additif $\mathbb{Z}/4Z$.

12. Déterminer les entiers x qui vérifient :

    (a) $x^3 \equiv 1 \pmod 7$.

    (b) $x^4 \equiv 1 \pmod{17}$.

    (c) $1 + x + x^2 + x^3 + x^4 \equiv 0 \pmod{31}$.

13. Résoudre les systèmes de congruences :

    (a) $\begin{cases} x \equiv 3 \pmod{37} \\ x \equiv 4 \pmod{52} \end{cases}$

    (b) $\begin{cases} x \equiv 21 \pmod{12} \\ x \equiv 12 \pmod{21} \end{cases}$

    (c) $\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 6 \pmod{8} \\ x \equiv -1 \pmod{15} \end{cases}$

14. Soit n un entier, $n > 1$. On dit que $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est un idempotent si $\overline{x}^2 = \overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$.

    (a) Soit $n = pq$ où p et q sont des nombres premiers. Combien y a-t-il d'idempotents dans $\mathbb{Z}/n\mathbb{Z}$?

    (b) Déterminer les idempotents de $\mathbb{Z}/n\mathbb{Z}$ pour $n = 5$, $n = 6$, $n = 10$, $n = 12$, $n = 15$.

    (c) Soit $n = p^k$, où p est un nombre premier. Quels sont les idempotents de $\mathbb{Z}/n\mathbb{Z}$?

    (d) Quel est le nombre des idempotents de $\mathbb{Z}/n\mathbb{Z}$ si n a exactement r diviseurs premiers ?

15. Déterminer les entiers m, n tels que $2^m \pm 3^n = 41$.