Université Bordeaux 1 — **MHT633 – Arithmétique et Cryptologie**
Mathématiques — Année 2008–2009

FEUILLE D'EXERCICES n° 3
Compléments d'arithmétique

Exercice 1 – [Théorème Chinois]
Dans le livre de Sun Zi, le Sunzi Suanjing datant du IIIe siècle, on trouve le problème suivant :

> Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste 2 soldats, rangés par 5 colonnes, il reste 3 soldats et, rangés par 7 colonnes, il reste 2 soldats ?

La résolution proposée par Sun Zi pour le problème des soldats est la suivante :

> Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute lui le produit du reste de la division par 5, c'est-à-dire 3, par 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2, par 15. Tant que le nombre est plus grand que 105, retire 105.

La solution n'explique pas très clairement la méthode utilisée. Nous allons formaliser les choses :

1) Soient a et $b \in \mathbb{Z}$ deux entiers non nuls premiers entre eux. Si $n \neq 0$, on note x_n la classe de x dans $\mathbb{Z}/n\mathbb{Z}$. Montrer que l'application

$$\begin{array}{rccc} \Phi\colon & \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & x_{ab} & \longmapsto & (x_a, x_b) \end{array}$$

est bien définie.

2) Montrer qu'il s'agit d'un isomorphisme d'anneaux et déterminer sa réciproque.

3) Généraliser à r entiers non nuls $a_1, a_2, \ldots, a_r$ premiers entre eux deux à deux.

4) Résoudre le problème de Sun Zi et retrouver la solution proposée.

5) Résoudre le problème suivant :

> Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et 6 d'entre eux sont tués. Un nouveau partage

donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, 6 pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Exercice 2 – [Indicatrice d'Euler]
Soit φ la fonction indicatrice d'Euler définie sur $\mathbb{Z}_{>0}$ par

$$\varphi(n) = |\{k \in \mathbb{Z}_{>0} \colon 1 \leqslant k \leqslant n \text{ et } \operatorname{pgcd}(k,n) = 1\}|\,.$$

1) Montrer que $\varphi(n)$ est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$.

2) Soit p un nombre premier et $k \in \mathbb{Z}_{>0}$. Calculer $\varphi(p)$ et $\varphi(p^k)$.

3) Se servir du théorème chinois pour établir que si

$$n = \prod_{i=1}^{r} p_i^{e_i}$$

est la décomposition en produit de facteurs premiers de n on a

$$\varphi(n) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

4) Soit n, $a \in \mathbb{Z}_{>0}$ tels que $\operatorname{pgcd}(a,n) = 1$. Montrer que

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Ce résultat généralise le petit théorème de Fermat.

5) En déduire une façon de calculer l'inverse de x_n dans $(\mathbb{Z}/n\mathbb{Z})^*$ (même notation que dans l'exercice 1), qui ne fasse pas appel à l'algorithme d'Euclide étendu. Application : calcul de l'inverse de 7_{15} dans $(\mathbb{Z}/15\mathbb{Z})^*$.

Exercice 3 – [Exponentiation binaire]

1) Montrer que 35 est inversible modulo 129.

2) Calculer l'inverse de 35 modulo 129 à l'aide de l'algorithme d'Euclide.

3) Calculer le maintenant par la méthode de l'exercice précédent.

4) Écrire un algorithme récursif permettant de calculer $a^k \pmod{n}$ de façon économique, en distinguant les cas k pair / impair, puis en se ramenant à un problème du même type après une mise au carré.

Exercice 4 – [Ordre d'un élément dans un groupe abélien fini]

Soit G un groupe abélien fini. On note multiplicativement sa loi de composition interne et e son élément neutre. On rappelle que l'ordre d'un élément g de G est le plus petit entier $k \geqslant 1$ tel que $a^k = e$. On pourra poser $|G| = n$.

1) Dans cette question (et uniquement dans celle-ci) on suppose G cyclique de générateur g. Quel est l'ordre d'un élément quelconque g^r ?

2) Montrer que si les ordres de a et $b \in G$ sont premiers entre eux, ab a pour ordre leur produit.

3) Soit $H = \langle a, b \rangle$ le sous-groupe de G engendré par deux éléments a et b. Montrer qu'il existe $g \in H$ d'ordre le ppcm des ordres de a et b.

[*Indication : noter* $\prod p_i^{e_i}$ *la décomposition en produit de facteur premiers du ppcm en question ; pour chaque* i*, déterminer un* $g_i \in H$ *d'ordre* $p_i^{e_i}$.]

4) Soit ω le ppcm des ordres des éléments de G. Déduire de la question précédente qu'il existe $g \in G$ d'ordre ω et que ω divise $|G|$.

5) En déduire que tout sous-groupe multiplicatif fini G d'un corps commutatif K est cyclique.
[*Indication : remarquer que tout* $x \in G$ *est racine de* $X^\omega - 1$ *et en déduire que* $\omega = |G|$.]

Exercice 5 – Travail dans $\mathbb{F}_{16}$

1) Trouver dans $\mathbb{F}_2[X]$ tous les polynômes irréductibles de degrés 1, 2, 3 et 4.

2) On considère le polynôme $P(X) = X^4 + X + 1$ qui est irréductible dans $\mathbb{F}_2[X]$ et l'on pose

$$\mathbb{F}_{16} = \mathbb{F}_2[X]/(P(X)),$$

qui est un corps à 16 éléments. Vérifier que $\omega = X \bmod P(X)$ engendre $\mathbb{F}_{16}^*$. On dressera la liste des puissances de ω sous la forme de 4-uplets $[\varepsilon_3, \varepsilon_2, \varepsilon_1, \varepsilon_0]$, où $\varepsilon_i \in \mathbb{F}_2$, représentant l'élément $\sum_{i=0}^{3} \varepsilon_i \omega^i$. Par exemple

$$\omega^5 = \omega^2 + \omega = [0, 1, 1, 0].$$

3) À l'aide de ce codage, coder $\omega^{57} \cdot \omega^{18}$ puis $\omega^{13} + \omega^{11} + \omega^8 + \omega^2 + 1$ et calculer les comme puissances de ω.

4) En déduire des règles de calcul simples et commencer à dresser les tables d'addition et de multiplication de $\mathbb{F}_{16}$.

5) Identifier un corps à 4 éléments dans $\mathbb{F}_{16}$.

6) À chaque indice i $(1 \leqslant i \leqslant 14)$ on associe j $(1 \leqslant j \leqslant 14)$ tel que

$$\omega^j = 1 + \omega^i.$$

Montrer qu'un tel j est bien défini et qu'alors on a $\omega^i = \omega^j + 1$.

7) On écrira alors $i \longleftrightarrow j$ et on parlera de correspondance de Zech. Dresser la liste des correspondances de Zech de $\mathbb{F}_{16}$.

8) Montrer que le recours à ces correspondances peut ramener le calcul de sommes de puissances de ω à celui beaucoup plus simple de produits de puissances de ω.