UNIVERSITÉ DE PARIS 7
Année 2000-2001, DEUG 2ème année
Groupes et arithmétique (MT282)

5 Etude des groupes $(\mathbf{Z}/n\mathbf{Z})^*$

5.1 Arithmétique

1. Quel est le dernier chiffre de 7777^{7777} ?
2. Quels sont les restes des divisions euclidiennes de 900^{2000} et de $101^{102^{103}}$ par 13 ?
3. Quel est le reste de la division euclidienne de $31^{32^{33}}$ par 7 ?
4. Quel est le reste de la division euclidienne de $100^{100^{100}}$ par 12 ?

5.2 Isomorphismes $(\mathbf{Z}/n\mathbf{Z}^*, \cdot) \simeq \oplus_i(\mathbf{Z}/n_i\mathbf{Z}, +)$

1. Quel est l'ordre de $(\mathbf{Z}/n\mathbf{Z})^*$ pour $n \in \{5, 8, 13, 19, 21, 25, 27, 33, 36\}$?
2. Lesquels de ces 9 groupes sont isomorphes deux-à-deux ?
3. Les groupes $(\mathbf{Z}/45\mathbf{Z})^*$ et $(\mathbf{Z}/56\mathbf{Z})^*$ sont-ils isomorphes ?

5.3 Algorithme de calcul

Soient $(G, \cdot)$ un groupe et g un élément de G d'ordre fini m. On veut calculer g^n pour un entier n que l'on suppose inférieur à m.

1. *Première méthode :* On calcule g^2, g^3, g^4, ... jusqu'à g^n. Combien d'opérations effectue-t-on alors ?
2. *Deuxième méthode :* On considère le développement en base 2 de n : $n = c_0 + c_1.2 + c_2.2^2 + \cdots + c_k.2^k$. Les c_i sont donc des entiers égaux à 0 ou 1 et k est la partie entière du logarithme en base 2 de n. On calcule g^2, $g^4 = (g^2)^2$, g^8, ... jusqu'à g^{2^k}.

   Exprimer g^n en fonction des g^{2^i} et des c_i pour $i = 0 \dots k$.
3. Combien effectue-t-on alors au maximum d'opérations dans G pour obtenir g^n ?
4. Calculer 9^{39} dans $\mathbf{Z}/83\mathbf{Z}$ puis 11^{23} dans $\mathbf{Z}/101\mathbf{Z}$.

5.4 Diviseurs de zéro

Soit A un anneau commutatif. On appelle un élément a de A *diviseur de zéro* s'il existe $b \in A$ non-nul tel que $ab = 0$.

1. Montrer qu'un élément inversible de A n'est pas un diviseur de zéro.
2. On pose maintenant $A = \mathbf{Z}/n\mathbf{Z}$, où n est un entier naturel non-nul. Si a n'est pas un diviseur de zéro de $\mathbf{Z}/n\mathbf{Z}$, montrer que l'ensemble $\{ab \mid b \in \mathbf{Z}/n\mathbf{Z}\}$ est en bijection avec $\mathbf{Z}/n\mathbf{Z}$.
3. En déduire que les éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$ sont les éléments qui ne sont pas des diviseurs de zéro.

5.5 Diviseurs premiers des nombres de Fermat

Soit n un entier naturel. On rappelle que le n-ème nombre de Fermat est l'entier $F_n = 2^{2^n} + 1$.

1. Soit p un nombre premier divisant F_n. Quelle est la classe de F_n dans $\mathbf{Z}/p\mathbf{Z}$?
2. Quel est l'ordre de 2 dans $\mathbf{Z}/p\mathbf{Z}$?
3. En déduire que 2^{n+1} divise $p-1$.

Remarque : Ainsi par exemple $641 = 10.2^6 + 1$ divise F_5, comme on l'a vu dans la feuille 1.

5.6 Carrés dans $\mathbf{Z}/p\mathbf{Z}$

Soient p un nombre premier impair, x un élément non-nul de $\mathbf{Z}/p\mathbf{Z}$.

1. Que vaut x^{p-1} ? Quel peut être l'ordre de $x^{\frac{p-1}{2}}$?
2. Quelles valeurs peut prendre $x^{\frac{p-1}{2}}$?
3. On dit qu'un élément x de $\mathbf{Z}/p\mathbf{Z}$ est un carré s'il existe $y \in \mathbf{Z}/p\mathbf{Z}$ tel que $x = y^2$. Quels sont les carrés de $\mathbf{Z}/13\mathbf{Z}$?
4. Que vaut $x^{\frac{p-1}{2}}$ si x est un carré ?
5. Soit x_0 un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$. Que vaut ${x_0}^{\frac{p-1}{2}}$?
6. Soit $x \in (\mathbf{Z}/p\mathbf{Z})^*$ tel que $x^{\frac{p-1}{2}} = 1$. En utilisant le fait que x_0 engendre $(\mathbf{Z}/p\mathbf{Z})^*$, montrer que x est un carré dans $\mathbf{Z}/p\mathbf{Z}$. En déduire la règle suivante :

   Un élément x de $(\mathbf{Z}/p\mathbf{Z})^*$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.
7. On considère le groupe multiplicatif $\{\pm 1\}$. Montrer que l'application

$$\begin{aligned} \varepsilon \ : (\mathbf{Z}/p\mathbf{Z})^* &\longrightarrow \{\pm 1\} \\ x &\longmapsto x^{\frac{p-1}{2}} \end{aligned}$$

   est un morphisme de groupe surjectif. En déduire l'ordre de son noyau puis le nombre de carrés de $(\mathbf{Z}/p\mathbf{Z})^*$.
8. Vérifier les deux questions précédentes en supposant $p = 7$.

5.7 Equations du second degré dans $\mathbf{Z}/n\mathbf{Z}$

1. Résoudre l'équation $x^2 + 4x - 1 = 0$ dans $\mathbf{Z}/11\mathbf{Z}$.
2. Montrer en utilisant l'exercice précédent que l'équation $x^2 + 5x + 2 = 0$ n'a pas de solution dans $\mathbf{Z}/11\mathbf{Z}$.
3. En utilisant le lemme chinois, résoudre l'équation $x^2 + 6x - 13 = 0$ dans $\mathbf{Z}/21\mathbf{Z}$.
4. Résoudre l'équation $x^2 + 3x + 2 = 0$ dans $\mathbf{Z}/6\mathbf{Z}$.
5. Résoudre l'équation $x^2 + 4x + 6 = 0$ dans $\mathbf{Z}/9\mathbf{Z}$.

5.8 Théorème de Wilson

Le but de ce problème est de montrer le théorème de Wilson :
Un entier $n > 1$ est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$.

1. Supposons d'abord que n n'est pas premier. Soit p un nombre premier divisant n. Quelle est la classe de $(n-1)!$ dans $\mathbf{Z}/p\mathbf{Z}$? En déduire que $(n-1)!$ ne peut être congru à -1 modulo n.

2. Réciproquement, si p est un nombre premier, montrer que pour tout entier x tel que $0 < x < p$, il existe un entier y tel que $0 < y < p$ et $xy \equiv 1 \pmod{p}$. Dans quel cas a-t-on $y = x$?

3. En déduire que $(p-1)! \equiv -1 \pmod{p}$ et conclure.

5.9 Racine carrée de -1

1. Soit p un nombre premier impair. Montrer que -1 est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si $p \equiv 1 \pmod{4}$.

2. Montrer que $[(\frac{p-1}{2})!]^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \pmod{p}$, puis calculer $[(\frac{p-1}{2})!]^2$ dans $\mathbf{Z}/p\mathbf{Z}$ en utilisant le théorème de Wilson.

3. Si $p \equiv 1 \pmod{4}$, donner une expression des racines carrées de -1.