Université de Paris 7 **2009-2010**
31UBMT42

Arithmétique I

Exercice I:

On considère le nombre $p = 2^3.277.797 + 1 = 1766153$. On effectue les calculs[1] suivants:

$$3^{883076} = -1[p], 2^{2216} = 1603914[p], 5^{6376} = 760770[p]$$

et l'on vérifie aussi que $2^{p-1}, 3^{p-1}, 5^{p-1}$ sont congrus à 1 modulo p.

1) Montrer que p est premier.

2) Donner un isomorphisme explicite de $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ vers $(\mathbb{Z}/p\mathbb{Z})^\times$

Exercice II:

On considère deux entiers a et b, on note d et m leur pgcd et ppcm. Comment ferait t'on pour expliciter un isomorphisme d'anneaux entre $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})$ et $(\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$?

Exercice III:

Soit G un groupe fini, et ρ un morphisme de G vers $GL_n(\mathbb{C})$. On note χ_ρ l'application de G dans $\mathbb{C}$ définie par: $\chi_\rho(g) = trace(\rho(g))$.

1) Que peut on dire de χ_ρ lorsque $n = 1$ et G abélien?

2) Si G est abélien et fini, montrer que χ_ρ est somme de n caractères. (Pour la définition donnée en cours).

3) Donner un exemple de groupe fini G tel que $\chi_\rho(g)$ ne soit pas une combinaison linéaire de morphismes de G vers $(\mathbb{C}^\times, .)$.

Exercice IV:

1) a) Pour $m \in \mathbb{Z}^*$, $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ est il toujours cyclique?

b) Si $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ est cyclique, quel est son nombre de générateurs (en fonction de ϕ)?

c) Pour $\alpha \in \mathbb{N}^*$, étudier si $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$ est cyclique.

2) Soit p un nombre premier impair, et α un entier supérieur ou égal à 2.

a) Calculer $\phi(p^\alpha)$.

b) Montrer que $\forall a \in \mathbb{Z}$ tel que p ne divise pas a, pour tout entier naturel n non nul, $1 + ap$ est d'ordre p^{n-1} modulo p^n.

3) a) En déduire que $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ est cyclique.

b) Que peut on dire de $\left(\mathbb{Z}/2p^\alpha\mathbb{Z}\right)^\times$?

4) a) Soit $G = G_1 \times G_2$ où les G_i sont des groupes de cardinal k_i. Montrer que si G est cyclique, alors k_1 et k_2 sont premiers entre eux.

b) En déduire que si $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ est cyclique, alors m vaut l'un des valeurs $1, 2, 4, p^\alpha, 2p^\alpha$.

Exercice V:

1) Donner explicitement un 2-Sylow de $(\mathbb{Z}/16\mathbb{Z})^\times$, et un sous groupe cyclique maximal.

2) Donner un isomorphisme de groupes: $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, +) \to ((\mathbb{Z}/16\mathbb{Z})^\times, .)$

3) Généraliser ce résultat à $(\mathbb{Z}/2^n\mathbb{Z})^\times$ pour $n \geq 3$.

4) a) Montrer que pour tout nombre premier impair, $X^4 + 1$ a 2 facteurs irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors qu'il est irréductible dans $\mathbb{Z}[X]$.

b) (Question facultative) Montrer que pour tout entier n non nul, $X^{2^n} + 1$ a 2 facteurs irréductibles dans $\mathbb{Z}/5\mathbb{Z}[X]$.

Exercice VI:

En étudiant $(n!)^2 + 1$, montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4

[1] On pourra essayer powmod(3,883076,1766153) sous le logiciel libre xcas (disponible à l'oral de l'agrégation): `http://www-fourier.ujf-grenoble.fr/~parisse/giac_fr.html`