UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille de TD 2

Exercice 1

On propose (encore !) une preuve, cette fois de dénombrement, du théorème d'Euclide. Supposons que l'ensemble des nombres premiers est fini,

$$\mathcal{P} = \{p_1, ..., p_k\},$$

1 Montrez que tout entier $n \geq 1$ s'écrit de manière unique

$$n = bc^2,$$

où b est sans facteur carré.

2 Montrez que le segment entier $[1, N]$ contient au plus $2^k\sqrt{N}$ nombres entiers.

3 Conclure

Exercice 2

Le but de l'exercice est de redémontrer l'équation satisfaite par la fonction caractéristique d'Euler :

$$\forall n \geq 1, \sum_{d|n} \varphi(d) = n.$$

1 Soit $G = \langle a \rangle$ un groupe cyclique d'ordre n muni d'un générateur a. Si $d|n$, montrez que les solutions de $x^d = 1$ sont $\{1, b, b^2, ..., b^{d-1}\}$ pour $b = a^{n/d}$.

2 Montrez que $b^r \in \langle b \rangle$ est d'ordre d ssi $(r, d) = 1$. En déduire que le nombre d'éléments de G ayant ordre d est $\varphi(d)$.

3 Conclure.

Exercice 3

Soit G un groupe abélien d'ordre n, tel que pour tout diviseur d de n, il y a au plus d solutions à l'équation $x^d = 1$. Montrez, en utilisant la structure des groupes abéliens finis, que G est alors cyclique.

Exercice 4

Structure des groupes $(\mathbf{Z}/2^e\mathbf{Z})^\times$.

1 Décrire $(\mathbf{Z}/2^e\mathbf{Z})^\times$ pour $e = 1, 2, 3$. Sont-ils cycliques ?

2 Montrez par récurrence que pour $n \geq 0$,

$$(1 + 4a)^{2^n} \equiv 1 + 2^{n+2}a \ (mod\ 2^{n+3}).$$

3 Montrez que pour $e \geq 3$, 5 est d'ordre 2^{e-2} dans $(\mathbf{Z}/2^e\mathbf{Z})^\times$.
4 En conclure que pour $e \geq 3$, $(\mathbf{Z}/2^e\mathbf{Z})^\times$ est isomorphe à $\{\pm 1\} \times \langle 5 \rangle$.

Exercice 5
1 Soit G un groupe abélien, a, b deux éléments d'ordres respectifs p, q, premiers entre eux : $(p, q) = 1$. Montrez que ab est d'ordre pq.
2 Soit G un groupe abélien fini. Si m désigne le ppcm des ordres des éléments de G, montrez qu'il existe un élément d'ordre m.
3 Soit K un corps, et G un sous-groupe fini de $K^\times$. On souhaite redémontrer le résultat (connu) que G est alors cyclique. Montrez que le ppcm de l'ordre des éléments de G est nécessairement $|G|$, puis conclure.

Exercice 6
Soit n un nombre de Carmichael. En particulier n est sans facteurs carré, produit d'au moins 2 premiers (en réalité, on peut montrer qu'il est produit d'au moins 3 premiers, et impair). On écrit $n - 1 = 2^s t$, où t est impair et $s \geq 1$. Pour $i \in \{0, .., s\}$, définissons

$$h_i : (\mathbf{Z}/n\mathbf{Z})^\times \to (\mathbf{Z}/n\mathbf{Z})^\times,$$

$$x \mapsto x^{2^i t}.$$

On pose enfin $K_i = Ker(h_i), I_i = Im(h_i)$.
1 Montrez que

$$K_0 \subsetneq K_1 \subset K_2 ... \subset K_s = (\mathbf{Z}/n\mathbf{Z})^\times.$$

2 Soit j le plus petit indice tel que $K_{j+1} = (\mathbf{Z}/n\mathbf{Z})^\times$. Si p est un facteur premier de n, écrivons $p-1 = 2^{s_p} t_p$ où t_p est impair. On rappelle que $p-1$ divise $n - 1$. Exprimer j en fonction des nombres s_p, puis montrez que $I_j \not\subset \{\pm 1\}$.
3 Montrez qu'au moins la moitié des éléments de $(\mathbf{Z}/n\mathbf{Z})^\times$ sont témoins de Miller-Rabin.

Exercice 7
Théorème de Wolstenholme. Pour $p > 3$ un nombre premier, on pose

$$S = 1 + \frac{1}{2} + ... + \frac{1}{p-1},$$

qui est un nombre rationnel.
1 Montrez que les entiers $a_1, ..., a_{p-2}$ défini par:

$$\prod_{i=1}^{p-1}(X - i) = (p-1)! + a_1 X + a_2 X^2 + ... + a_{p-1} X^{p-2} + X^{p-1},$$

sont tous divisibles par p.
2 Montrez que $S = \frac{-a_1}{(p-1)!}$.
3 Montrez que le numérateur de S est divisible par p^2.