Examen du 5 juin 2003

Durée : 3 heures

Les documents ne sont pas autorisés

Exercice 1.

Notations.

Soit p un nombre premier. On note $\mathbf{F}_p$ le corps à p éléments.

Les lettres m, n et d désignent des entiers ≥ 1.

On note E_n l'ensemble des polynômes unitaires irréductibles de $\mathbf{F}_p[X]$ de degré n. On désigne par $\psi(n)$ le nombre de polynômes unitaires irréductibles de $\mathbf{F}_p[X]$ de degré n (c'est-à-dire le nombre d'éléments de E_n) et par $\pi(n)$ le nombre de polynômes unitaires irréductibles de $\mathbf{F}_p[X]$ de degré $\leq n$ (c'est-à-dire le nombre d'éléments de $\bigcup_{1\leq m\leq n} E_m$).

On désigne par $\mu(n)$ la fonction de Möbius.

a) Soit f un polynôme irréductible dans $\mathbf{F}_p[X]$ de degré m. Montrer que f divise $X^{p^n}-X$ dans $\mathbf{F}_p[X]$ si et seulement si m divise n.

b) En déduire
$$X^{p^n}-X=\prod_{d|n}\prod_{f\in E_d} f(X)\in \mathbf{F}_p[X].$$

c) Vérifier
$$p^n=\sum_{d|n} d\psi(d).$$

d) Montrer
$$\psi(n)=\frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}.$$

e) Montrer
$$\pi(n)\sim\frac{p}{p-1}\cdot\frac{p^n}{n}\qquad\text{pour}\qquad n\to\infty.$$

Estimer le terme d'erreur.

Exercice 2.

Notations.

Soit p un nombre premier. On note $\mathbf{F}_p$ le corps à p éléments.

La notation $\Re s$ désigne la partie réelle d'un nombre complexe s.

On désigne par E l'ensemble des polynômes unitaires irréductibles de $\mathbf{F}_p[X]$ et par H l'ensemble des polynômes unitaires de $\mathbf{F}_p[X]$. Pour $h \in H$ on note $\deg h$ le degré de h. Quand s est un nombre complexe de partie réelle > 1, on pose

$$Z(s) = \sum_{h \in H} \frac{1}{p^{s \deg h}} \cdot$$

a) Montrer que la série $Z(s)$ est normalement convergente sur tout compact du demi-plan $\Re s > 1$. La fonction Z est-elle holomorphe sur ce demi-plan $\Re s > 1$?

b) Vérifier, pour $\Re s > 1$,

$$Z(s) = \frac{1}{1 - p^{1-s}} \cdot$$

En déduire que la fonction $Z(s)$ se prolonge en une fonction méromorphe sur $\mathbf{C}$. Quels sont ses zéros? Ses pôles? Ses résidus?

c) Pour $\Re s > 1$, écrire de la manière la plus simple possible $Z(s)$ sous la forme d'un produit infini indexé par les éléments de E.