SUITES BINAIRES PARFAITES

Une suite parfaite binaire de longueur n est une application f de $\mathbf{Z}/n\mathbf{Z}$ dans ± 1 vérifiant :

$$\sum_{j-i\equiv t} f(i)f(j) = \begin{cases} n, & t \equiv 0 \pmod{n}; \\ 0, & \text{sinon.} \end{cases}$$

Les congruences prises modulo n. L'objectif de l'exercice est de montrer l'inexistence des suites binaires dont la longueur est une puissance de 2 assez grande. Ainsi, dans la suite f désigne une suite parfaite binaire de longueur $n = 2^m$, $m \geq 1$.

1. Caractérisation spectrale

On note $f(X)$ le polynôme $\sum_{i=0}^{n-1} f(i)X^i$. Pour $z \in \mathbf{C}$, on note z^* le conjugué de z. Montrer que si ζ est une racine n-ième de l'unité dans $\mathbf{C}$ alors

$$f(\zeta)f(\zeta)^* = n.$$

2. Propriétés arithmétiques

On note ζ_n la racine n-ième primitive standard dans $\mathbf{C}$, c'est le nombre complexe $\zeta_n = \exp(2i\pi/n)$. On note K le corps cyclotomique $\mathbf{Q}(\zeta_n)$, et on note A l'anneau des entiers de K, on sait que $A = \mathbf{Z}[\zeta_n]$. On rappelle que A est un anneau de Dedekind dans lequel tout idéal se factorise en un produit d'idéaux premiers. En particulier, si p désigne un nombre premier alors il existe g idéaux premiers P_i tels que :

$$pA = \prod_{i=1}^{g} P_i^e, \quad f = \dim_{\mathbf{F}_p} A/P_i, \quad efg = [K : \mathbf{Q}].$$

où les anneaux A/P_i sont finis. Par ailleurs, le groupe de Galois de $K/\mathbf{Q}$ agit transitivement sur l'ensemble des idéaux premiers contenant p.

(1) Quelle est la nature des anneaux A/P_i ?
(2) Donner le cardinal de A/P_i en fonction de p et f.

3. Factorisation de 2

On note $\wp$ l'idéal principal engendré par $1 + \zeta_n$.

(1) Quel est le polynôme minimal de ζ_n ?
(2) Montrer l'égalité d'idéaux $2A = \wp^{2^{m-1}}$.
(3) Quel est le groupe de décomposition de $\wp$?

4. Divisibilité

Soit $a(X) \in \mathbf{Z}[X]$ un polynôme de degré n. On considère un entier naturel d divisant $a(\zeta_n)$ dans A sachant que $a(\zeta_n) \neq 0$.

(1) Montrer que $d \leq 2 \sup_i |a_i|$.
(2) Préciser ce résultat dans le cas où les coefficients de a sont positifs.

5. Conclusion

Aprés avoir remarqué que la conjugaison complexe est dans le groupe de décomposition de P. Montrer si f est parfaite alors

$$f(\zeta_n)A = \wp^{n/2}. \quad \text{(égalité d'idéaux)}$$

Montrer alors l'inexistence des suites parfaites binaires de longueurs $n = 2^m$ pour m assez grand.