Sommes de Gauss

Léo Théodon Malo Cossec

Université de Rennes 1

Jeudi 06 mai 2010

Plan

Symbole de Legendre

Définition

Soient p un nombre premier et n un entier relatif. On note :

1. $\left(\frac{n}{p}\right) = 0$ si p divise n.
2. $\left(\frac{n}{p}\right) = 1$ si n est un résidu quadratique modulo p.
3. $\left(\frac{n}{p}\right) = -1$ si n n'est pas un résidu quadratique modulo p.

L'expression $\left(\frac{n}{p}\right)$ s'appelle le symbole de Legendre.

Symbole de Legendre

Propriété

Propriété

Si q ne divise pas $a \in \mathbb{Z}$, alors $a^{(q-1)/2} \equiv \left(\frac{a}{q}\right) \ mod \ q$.

Caractères

Soit G un groupe abélien fini multiplicatif.

Définition

On appelle caractère multiplicatif de G tout homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^*$ des nombres complexes.

Sommes de Gauss

Première définition

Définition

Soit p un nombre premier impair, et soit $a \in \mathbb{F}_p$. On appelle *Somme de Gauss associée au caractère multiplicatif* χ *selon* a la somme suivante :

$$\mathcal{G}(\chi, a) = \sum_{x \in \mathbb{F}_p} \chi(x) e^{2i\pi ax/p}.$$

Sommes de Gauss
Propriétés

Propriétés

Les sommes $\mathcal{G}(\chi, a)$ vérifient les formules suivantes :

1. $\mathcal{G}(\chi, a) = \overline{\chi}(a)\mathcal{G}(\chi, 1)$.
2. $|\mathcal{G}(\chi, a)|^2 = p$.
3. $\mathcal{G}(\chi, 1) = \chi(-1)\mathcal{G}(\overline{\chi}, a)$.

Sommes de Gauss

Seconde définition

Définition

Soient p et q deux nombres premiers impairs distincts, et α une racine primitive p-ième de l'unité dans une extension de $\mathbb{F}_q$. On appelle alors *Somme de Gauss dans* $\mathbb{F}_q(\alpha)$ la somme suivante :

$$\tau = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \alpha^x$$

Sommes de Gauss
Propriétés

Propriétés

La somme τ vérifie les égalités suivantes.

1. $\tau^2 = \left(\frac{-1}{p}\right) p.$
2. $\tau^{q-1} = \left(\frac{q}{p}\right).$

Plan

Loi de réciprocité quadratique

Théorème

Théorème

Soient p et q deux nombres premiers impairs distincts. On a :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Loi de réciprocité quadratique

Preuve

1. $\left(\frac{p}{q}\right) = p^{(q-1)/2} = \left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2}$

Loi de réciprocité quadratique

Preuve

1. $\left(\frac{p}{q}\right) = p^{(q-1)/2} = \left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2}$
2. $\left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2} = (-1)^{(q-1)(p-1)/4}\tau^{q-1}$

Loi de réciprocité quadratique

Preuve

1. $\left(\frac{p}{q}\right) = p^{(q-1)/2} = \left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2}$
2. $\left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2} = (-1)^{(q-1)(p-1)/4}\tau^{q-1}$
3. $(-1)^{(q-1)(p-1)/4}\tau^{q-1} = (-1)^{(q-1)(p-1)/4}\left(\frac{q}{p}\right)$

Loi de réciprocité quadratique

Preuve

1. $\left(\frac{p}{q}\right) = p^{(q-1)/2} = \left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2}$
2. $\left(\left(\frac{-1}{p}\tau^2\right)\right)^{(q-1)/2} = (-1)^{(q-1)(p-1)/4}\tau^{q-1}$
3. $(-1)^{(q-1)(p-1)/4}\tau^{q-1} = (-1)^{(q-1)(p-1)/4}\left(\frac{q}{p}\right)$
4. $\left(\frac{p}{q}\right) = (-1)^{(q-1)(p-1)/4}\left(\frac{q}{p}\right)$

Théorème de Chevalley-Warning

Théorème

Soit $\mathbb{K} = \mathbb{F}_q$ un corps fini de caractéristique p. Si $P \in \mathbb{K}[x_1, ..., x_n]$, avec $deg(P) < n$, alors

$$Card\{x \in \mathbb{K}^n | P(x) = 0\} \equiv 0 \ mod \ p.$$

Nombre de solutions d'une forme quadratique

Théorème

Soit Q une forme quadratique en n variables, non dégénérée, à coefficients dans $\mathbb{F}_p$ (où $p \neq 2$), alors :

$$Card\{x \in \mathbb{F}_p^n \mid Q(x) = 0\} = p^{n-1} + \varepsilon(p-1)p^{\frac{n}{2}-1}$$

avec

$$\varepsilon = \begin{cases} 0 & si\ n\ est\ impair \\ \left(\dfrac{(-1)^{n/2} D_Q}{p}\right) & si\ n\ est\ pair \end{cases}$$

Plan

Théorème de Gauss

Définition

Définition

Un nombre de Fermat est un nombre p tel qu'il existe un $n \in \mathbb{N}$ pour lequel $p = 2^{2^n} + 1$.

Théorème de Gauss

Théorème

Théorème

Les polygones réguliers constructibles sont ceux dont le nombre de côtés n est de la forme 2^α, $\alpha \geq 2$ ou de la forme $2^\alpha p_1 p_2 ... p_r$ où les p_i sont des nombres premiers de Fermat.

Préliminaires
Définition

Définition

Un nombre $\alpha \in \mathbb{R}$ est dit constructible si il existe des sous-corps de $\mathbb{C} = K_0 \subset K_1 \subset K_2 \subset ... \subset K_n$, tels que $\alpha \in K_n$ et $K_i = K_{i-1}(\sqrt{\alpha_{i-1}})$.

Préliminaires
Lemmes

Lemme

Si m et n sont premiers entre eux, l'angle de mesure $\frac{\hat{2\pi}}{mn}$ est constructible si et seulement si $\frac{\hat{2\pi}}{n}$ et $\frac{\hat{2\pi}}{m}$ le sont.

Préliminaires
Lemmes

Lemme

Si $n \geq 3$ se décompose en facteurs premiers de la façon suivante

$$n = p_1^{\alpha_1} ... p_k^{\alpha_k},$$

le polygone régulier à n côtés est constructible si et seulement si les angles $\frac{\hat{2\pi}}{p_1^{\alpha_1}}, ..., \frac{\hat{2\pi}}{p_k^{\alpha_k}}$ le sont aussi.

Préliminaires
Théorème

Théorème

1. Les angles de la forme $\frac{\hat{2\pi}}{2^\alpha}$ sont constructibles.
2. Si p est premier impair et $\frac{\hat{2\pi}}{p^\alpha}$ est constructible, alors $\alpha = 1$ et p est un nombre de Fermat.

Fin de la preuve par les Sommes de Gauss

Définition

Définition (Somme de Jacobi)

Soient χ et λ des caractères sur $\mathbb{F}_p$. On note

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b).$$

Fin de la preuve par les Sommes de Gauss

Propriétés

Propriété

Soient χ et λ des caractères non-triviaux sur $\mathbb{F}_p$. Si $\chi\lambda \neq 1$, alors :

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Propriété

Supposons que $p \equiv 1\ (n)$ et que χ est un caractère d'ordre $n > 2$. Alors :

$$g(\chi)^n = \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2)...J(\chi, \chi^{n-2}).$$

Fin de la preuve par les Sommes de Gauss

Théorème

Théorème

Si p est un nombre de Fermat premier, alors ζ_p est constructible.

Fin de la preuve par les Sommes de Gauss

Démonstration

Soit $g(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta_p^t$ la Somme de Gauss associée à χ. Alors

$$\begin{aligned} \sum_{\chi \in \hat{\mathbb{F}_p^*}} g(\chi) &= \sum_{t=0}^{p-1} \left(\sum_{\chi \in \hat{\mathbb{F}_p^*}} \chi(t) \right) \zeta_p^t \\ &= 1 + (p-1)\zeta_p. \end{aligned}$$

Ainsi, $\zeta_p = (p-1)^{-1}(-1 + \sum_{\chi \in \hat{\mathbb{F}_p^*}} g(\chi))$, et on a que :

$$g(\chi)^{2m} = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)...J(\chi,\chi^l)$$

Fin de la preuve par les Sommes de Gauss

Le Théorème de Gauss est prouvé.