Année 2024-2025

L3 (S6) – Méthodes analytiques dans l'arithmétique.

Contrôle continu.

1 avril 2026

Durée 1 heure. Utilisation des documents autorisée, mais pas encouragée.

Exercice 1.

Exprimer la somme

$$\sum_{k=0}^{p-1} \zeta^{k^2}$$

(où $\zeta^p = 1$, $\zeta \neq 1$) en termes de sommes de Gauss $\tau(\chi) = \sum_{k=0}^{p-1} \chi(k)\zeta^k$.

Exercice 2.

Caractériser les nombres premiers impairs p pour lesquels l'équation

$$x^2 + x + 1 = 0 \mod p$$

a une solution.

Exercice 3.

Calculer $\left(\frac{449}{373}\right)$.

Exercice 4.

Soient p un nombre premier et n un diviseur de $p-1$ et $a \in (\mathbb{Z}/p\mathbb{Z})^\times$

a. Montrer que l'équation $x^n \equiv a \not\equiv 0 \mod p$ a une solution si et seulement si $a^{\frac{p-1}{n}} \equiv 1 \mod p$.

b. Combien de racines peut avoir l'équaton $x^n = a$.

c. Pour $a \in \mathbb{Z}/p\mathbb{Z}$ soit $N(a)$ le nombre de solution de l'équation $x^n \equiv a \mod p$. Montrer que

$$N(a) = \sum_{\chi \mid \chi^n = \varepsilon} \chi(a).$$

Exercice 4 bis

Soit $\omega = e^{2\pi i/3}$ et $p > 3$ un nombre premier

a. Calculer $(2\omega + 1)^2$.

b. Calculer $(2\omega + 1)^p$ modulo p.

c. En déduire l'expression pour le symbole de Legendre $\left(\frac{-3}{p}\right)$.

Correction :

1.
$$\sum_{k=0}^{p-1}\zeta^{k^2}=\sum_{k=1}^{p-1}\left(1+\left(\frac{k}{p}\right)\right)\zeta^k=\sum_{k=0}^{p-1}\zeta^k+\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)\zeta^k=\tau(\chi)$$

où $\chi(x)=\left(\frac{x}{p}\right)$.

2.

$x^2+x+1=(x-1/2)^2+3/4$ donc l'équation est soluble si $-3/4$ est un carré modulo p.

$$\left(\frac{-3/4}{p}\right)=(-1)^{(p-1)/2}\left(\frac{3}{p}\right)\left(\frac{2}{p}\right)^2=\left(\frac{p}{3}\right)=\begin{cases}0 & \text{si } p=0 \bmod 3\\ 1 & \text{si } p=1 \bmod 3\\ -1 & \text{si } p=2 \bmod 3\end{cases}$$

Donc l'équation a deux solution modulo p si $p\equiv 1 \mod 3$ et une solution si $p=3$.

3. $\left(\frac{449}{373}\right)=\left(\frac{76}{373}\right)=\left(\frac{2}{373}\right)^2\left(\frac{19}{373}\right)=\left(\frac{373}{19}\right)=\left(\frac{12}{19}\right)=\left(\frac{2}{19}\right)^2\left(\frac{3}{19}\right)=-\left(\frac{19}{3}\right)=-\left(\frac{1}{3}\right)=-1$.
On a utilisé que $373\equiv 1 \bmod 4$ et $19\equiv 3 \bmod 4$.

4a. Soit g un générateur du groupe $\mathbb{Z}/p\mathbb{Z}$ et soit $a=g^k$ et $x=g^l$ où $k,l\in\mathbb{Z}/(p-1)\mathbb{Z}$. Donc l'équation peut être réécrit comme $g^nl=g^k$ équivalente à $nl\equiv k \bmod (p-1)$ qui a solutions si et seulement si k est divisible par n. Donc $a^{\frac{p-1}{n}}=g^{\frac{k(p-1)}{n}}$ et $\frac{k(p-1)}{n}$ est divisible par $(p-1)$ si et seulement si n divise k.
4b. Si n divise k il y a n solutions : $g^{\frac{k}{n}}, g^{\frac{k+p-1}{n}},\dots g^{\frac{k+(n-1)(p-1)}{n}}$. Si $a=0$ le nombre de racines et évidemment 1.
4c. Il y a exactement n caractères tels que $\chi^n=1$ (car le groupe de caractères est isomorphe à $(\mathbb{Z}/p\mathbb{Z})$ et l'équation $x^n=1$ à une solution). Si $\chi^n=\varepsilon$ et si $a=x^n$ évidemment $\chi(a)=\chi(x^n)=\chi^n(a)=1$. Donc $\sum_{\chi|\chi^n=\varepsilon}\chi(a)=n$.

Si $a^{\frac{p-1}{n}}\neq 1$ il existe un caractère χ_0 tel que $\chi_0(a^{\frac{p-1}{n}})\neq 1$. Donc le caractère $\chi_1=\chi_0^{\frac{p-1}{n}}$ est tel que $\chi_1^n=\varepsilon$ et $\chi_1(a)\neq 1$. Donc $0=(\chi_1(a)-1)\sum_{\chi|\chi^n=\varepsilon}\chi(a)$ et donc $\sum_{\chi|\chi^n=\varepsilon}\chi(a)=0$.
4'a. $(2\omega+1)^2=4\omega^2+4\omega+4-3=-3$ car $\omega^2+\omega+1=0$.
4'b. Modulo p on a $(2\omega+1)^p=2^p\omega^p+1^p=2\omega^p+1=\begin{cases}2\omega+1 \text{ si } p=1 \mod 3\\ 2\omega^2+1=2(-\omega-1)+1=-2\omega-1 \text{ si } p=2 \mod 3\end{cases}$
4'c. $\left(\frac{-3}{p}\right)=(-3)^{(p-1)/2}=(2\omega+1)^{p-1}$. Donc $\left(\frac{-3}{p}\right)(2\omega+1)=(2\omega+1)^p$. Alors $\left(\frac{-3}{p}\right)=\begin{cases}1 \text{ si } p=1 \mod 3\\ -1 \text{ si } p=2 \mod 3\end{cases}$.