Année 2024-2025

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

**Contrôle continu.**

1 avril 2025

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

### Exercice 1.

Caractériser les nombres premiers $p$ pour lesquels l'équation

$$x^2 = 7 \mod p$$

a une solution.

### Exercice 2.

Calculer $\left(\frac{345}{223}\right)$.

### Exercice 3.

Soit $f(x) = \begin{cases} 1 \text{ si } n = 4 \mod 7 \\ 0 \text{ sinon} \end{cases}$. Decomposer $f(x)$ en combinaison linéaire de

a. caractères additifs $\rho_k(x) = e^{2\pi i k x/7}$, $k = 0, \dots 6$.

b. caractères multiplicatifs $\chi_l(x)$ définis par $\chi_l(3) = e^{2\pi i l/6}$, $l = 0, \dots, 5$.
et multiplicatifs modulo 7.

### Exercice 4.

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.

$$\left(\frac{7}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{7}\right) = \left\{\begin{array}{rl} 1 & \text{si } p = 1 \mod 4 \\ -1 & \text{si } p = 3 \mod 4 \end{array}\right\}\left\{\begin{array}{rl} & 1 \text{ si } p = 1,2,4 \mod 7 \\ -1 & \text{si } p = 3,5,6 \mod 7 \end{array}\right\} =$$

$$= \left\{\begin{array}{rl} 1 & \text{si } p = 1,3,9,19,25,27 \mod 28 \\ -1 & \text{si } p = 5,11,13,15,17,23 \mod 28 \end{array}\right.$$

2. $\left(\frac{345}{223}\right) = \left(\frac{122}{223}\right) = \left(\frac{2}{223}\right)\left(\frac{61}{223}\right) = \left(\frac{223}{61}\right) = \left(\frac{40}{61}\right) = \left(\frac{2}{61}\right)^3\left(\frac{5}{61}\right) = -\left(\frac{61}{5}\right) = -1$. On a utilisé que $223 \equiv 7 \mod 8$, $61 \equiv 1 \mod 4$ et $61 \equiv 5 \mod 8$.

3a. $f(x) = \sum_{k=0}^{6} \frac{1}{p} e^{-8\pi ik/7}\rho_k(x)$.

3b. $f(x) = \sum_{l=0}^{5} \frac{1}{p-1} e^{-4\pi ik/3}\chi_l(x)$.

4a. $(2\omega+1)^2 = 4\omega^2 + 4\omega + 4 - 3 = -3$ car $\omega^2 + \omega + 1 = 0$.

4b. Modulo $p$ on a $(2\omega+1)^p = 2^p\omega^p + 1^p = 2\omega^p + 1 = \left\{\begin{array}{l} 2\omega + 1 \text{ si } p = 1 \mod 3 \\ 2\omega^2 + 1 = 2(-\omega - 1) + 1 = -2\omega - 1 \text{ si } p = 2 \mod 3 \end{array}\right.$

4c. $\left(\frac{-3}{p}\right) = (-3)^{(p-1)/2} = (2\omega+1)^{p-1}$. Donc $\left(\frac{-3}{p}\right)(2\omega+1) = (2\omega+1)^p$. Alors $\left(\frac{-3}{p}\right) = \left\{\begin{array}{l} 1 \text{ si } p = 1 \mod 3 \\ -1 \text{ si } p = 2 \mod 3 \end{array}\right.$.