Devoir maison no.2, Contrôle Continu M1 4023 Algorithmique Algébrique, Sorbonne Université 2020/2021

Date : distribué le 8 avril 2021, à rendre sur Moodle avant le 15 avril à 23h59.
Enseignant : Pierre CHAROLLOIS, Pierre-Vincent KOSELEFF.
Vous pouvez, si vous le souhaitez, faire vérifier vos calculs au moyen d'un logiciel de calcul formel (par exemple Sage, disponible sur le site https://jupyter.math.upmc.fr/).

Exercice 1 (sommes de Dedekind)

Soit $\sigma \in M_2(\mathbb{Z})$ une matrice de rang 2.

a) Montrer que les colonnes de σ engendrent un sous-groupe $\sigma\mathbb{Z}^2$ de $\mathbb{Z}^2$ d'indice fini, égal à $|\det(\sigma)|$.

b) Soit $\sigma_0 = \begin{pmatrix} 11 & 4 \\ 7 & 3 \end{pmatrix}$. Trouver, en expliquant les calculs, des matrices $E, F \in GL_2(\mathbb{Z})$ et D diagonale avec $E\sigma_0 F = D$.

c) Déterminer un système de représentants explicite des classes du groupe quotient $\mathbb{Z}^2/\sigma_0\mathbb{Z}^2$.

d) On note $<,>$ le produit scalaire usuel sur $\mathbb{R}^2$, et σ^t la transposée de $\sigma \in M_2(\mathbb{Z})$. Montrer que pour tout $h \in \mathbb{Z}^2$,

$$\sum_{r \in \mathbb{Z}^2/\sigma\mathbb{Z}^2} \exp(2i\pi < \sigma^{-1}r, h >) = \begin{cases} \det(\sigma) & \text{si } h \in \sigma^t\mathbb{Z}^2 \\ 0 & \text{si } h \notin \sigma^t\mathbb{Z}^2. \end{cases} \tag{1}$$

e) On rappelle (Dirichlet) que pour $0 < v < 1$,

$$\lim_{N\to\infty} \sum_{m=-N}^{N} \frac{\exp(-2i\pi vm)}{t+m} = 2i\pi \frac{\exp(2i\pi vt)}{\exp(2i\pi t) - 1}.$$

Démontrer que la somme

$$\frac{1}{\pi^2} \sum_{0 \neq n \in \mathbb{Z}} \frac{\exp(2i\pi nv)}{n^2} \tag{2}$$

est un nombre rationnel lorsque v est un nombre rationnel.

f) Déduire des questions précédentes que

$$\sum_{(m,n)\in\mathbb{Z}^2, (11m+7n)(4m+3n)\neq 0} \frac{1}{(11m+7n)^2(4m+3n)^2} = \pi^4\lambda,$$

pour un nombre rationnel λ que l'on pourra déterminer. Quel est son dénominateur ? Généraliser.

Exercice 2 (factorisation)

Soit $f(x) = x^5 + 100x^4 + 2521x^3 + 78641x^2 + 197118x + 392863$ un polynôme de $\mathbb{Z}[x]$, et $\tilde{f}$ son image dans $\mathbb{F}_5[x]$.

a) Factoriser $\tilde{f}$ en un produit de facteurs irréductibles dans $\mathbb{F}_5[x]$.

b) Démontrer que f ne possède pas de racine rationnelle.

c) Soit g un facteur irréductible de f dans $\mathbb{Z}[x]$. Donner une majoration des coefficients de g.

d) Au moyen du relevé de Hensel, déduire des questions précédentes la factorisation de f dans $\mathbb{Z}[x]$ en facteurs irréductibles. (On détaillera les étapes du calcul).

Exercice 3 (résultant) :

Soit $P(x, y) = x^3 - y^2 + 1$ et $Q(x, y) = x^2 + y^2 + xy - 1$.

a) Calculer le résultant, en y, $\mathrm{Res}_y(P, Q) \in \mathbb{Z}[x]$.

b) Déterminer tous les couples $(x_i, y_i) \in \mathbb{Q}^2$ de nombres rationnels qui sont solutions du système

$$\left\{ \begin{array}{l} P(x, y) = 0 \\ Q(x, y) = 0. \end{array} \right. \tag{3}$$

Combien ce système possède-t'il de solutions rationnelles ?

c) Soit $p = 11$. A l'aide des questions a) et b), déterminer toutes les paires $(x', y') \in \mathbb{F}_p \times \mathbb{F}_p$ qui sont solutions du système

$$\left\{ \begin{array}{l} P(x', y') = 0 \\ Q(x', y') = 0. \end{array} \right. \tag{4}$$

Combien ce système possède-t'il de solutions dans $\mathbb{F}_p$?

d) (question bonus). Même question que la précédente, mais pour $p = 31$. Expliquez.