

Examen Master 2, Parcours Agrégation Option C

Mardi 18 avril 2017. CORRIGE.

Exercice 1.1. — Nombre d'or modulo p

- On a $\left(\frac{5}{p}\right) = (-1)^{\frac{(5-1)(p-1)}{4}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$. Les carrés de $(\mathbb{F}_5)^*$ sont ± 1 , d'où le résultat.
- Si $p = 5$ alors $P = (X - 3)^2$. Si $p = 2$, $P = X^2 + X + 1$ est irréductible. Sinon, $P = (X - 1/2) - 5/4$. P est scindé si et seulement si $p = \pm 1 \pmod{5}$. Puisque p est impair alors $p = \pm 1 \pmod{10}$.
- (a) p est impair et premier avec 10 donc $p \equiv \pm 3 \pmod{10}$.
(b) Il suffit de prendre une racine de Φ_{10} qui est irréductible dans $\mathbb{F}_p[X]$. Sinon, si $p \equiv \pm 3 \pmod{10}$, alors $10 \mid p^2 + 1 \mid p^4 - 1$. Une extension de degré 4 de $\mathbb{F}_p$ contient une racine d'ordre 10.
(c) β est d'ordre 10 donc β^5 est d'ordre 2 et $\beta^5 = -1$.
- (a) On a $\alpha^2 - \alpha - 1 = (\beta + 1/\beta)^2 - (\beta + 1/\beta) = (\beta^4 - \beta^3 + \beta^2 - \beta + 1)/\beta^2 = 0$. Donc α est racine de P .
(b) On a toujours $(x + y)^p \equiv x^p + y^p \pmod{p}$, donc $\alpha^p = (\beta + \beta^{-1})^p = \beta^p + \beta^{-p} = \beta^{\pm 3} + \beta^{\mp 3}$ car $\beta^{10} = 1$. Donc $\alpha^p = \beta^3 + \beta^{-3} = \beta^3 - \beta^2$ car $\beta^5 = -1$.
(c) On a alors $\alpha^{p+1} = (\beta^3 - \beta^2)(\beta + \beta^{-1}) = -1$.

Exercice 1.2. — Suite de Fibonacci

- On sait que $F_n = \lambda \varphi^n + \mu (-1/\varphi)^n \sim \lambda \varphi^n$. Mais alors $\log F_n \underset{n \rightarrow \infty}{\sim} n \log \varphi$.
(a) Démonstration par récurrence sur n . Si $(u_n, v_n) = (F_{n+1}, F_n)$ alors $u_{n+1} = F_{n+2}$ et $v_{n+1} = u_n = F_{n+1}$.
(b) On peut calculer $u_{k+1} = u_k + v_k$ en additionnant deux entiers de taille $O(k)$ donc en $K \cdot k = O(k)$ opérations binaires. On calcule le couple (u_n, v_n) en $\sum_{k=1}^n K \cdot k = O(n^2)$ opérations. On peut calculer F_n en $O(n^2)$ opérations binaires.
- On peut calculer la suite $(u_n \pmod{p}, v_n \pmod{p})$ en n additions dans $\mathbb{F}_p$, donc en $O(n \log p)$ opérations.
- (a) Si $p = 2$, on obtient 0, 1, 1, 0, 1, donc $(f_3, f_4) = (f_0, f_1)$. f_n est de période 3.
(b) Si $p = 5$, on obtient 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, donc $(f_{20}, f_{21}) = (f_0, f_1)$. f_n est de période 20.
(c) Si $p = 11$, on obtient 0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, donc $(f_{10}, f_{11}) = (f_0, f_1)$. f_n est de période 10.
(d) Si $p = 3$, on obtient 0, 1, 1, 2, 0, 2, 2, 1, 0, 1, donc $(f_8, f_9) = (f_0, f_1)$. f_n est de période 8.
- (a) Posons $g_n = \frac{\alpha}{\alpha^2 + 1} (\alpha^n - (-1)^n \alpha^{-n})$. On a alors $g_0 = 0$ et $g_1 = \frac{\alpha}{\alpha^2 + 1} (\alpha + \alpha^{-1}) = 1$. D'autre part g_n vérifie la même relation de récurrence que f_n donc $f_n = g_n$ pour tout n (par récurrence immédiate).
(b) On peut calculer α^n et α^{-n} en $O(\log n)$ opérations arithmétiques dans $\mathbb{F}_p$, en utilisant l'exponentiation dichotomique. Donc en $O(\log n (\log p)^2)$ opérations binaires.
- (a) En utilisant la question précédente, α^n est périodique (de période divisant $p - 1$ si $p \equiv \pm 1 \pmod{10}$ et de période divisant $2(p + 1)$ si $p \equiv \pm 3 \pmod{10}$, ou de période finie dans les autres cas ($p = 2, 5$).
(b) Soit $T = (p - 1)$ ou $T = 2(p + 1)$. Pour calculer f_n , il suffit de calculer $m = n \pmod{T}$ en $O(\log n \log T) = O(\log n \log p)$ opérations binaires puis f_m en $O(m \log p) = O(T \log p) = O(p \log p)$ opérations binaires.

Exercice 1.3. — Inégalité de Hadamard

1. M est une matrice symétrique positive donc $(x|Mx) \geq 0$.

(a) On a $(e_i|Me_i) = M_{i,i} \geq 0$.

(b) $M \geq 0$ donc $0 \leq \det M$. M est diagonalisable de valeurs propres réelles positives $\lambda_1, \dots, \lambda_n$. Si $\det M = 0$, l'inégalité est vraie, sinon $-\ln$ est convexe donc

$$-\ln\left(\sum \frac{1}{n} \lambda_i\right) \leq \sum -\frac{1}{n} \ln \lambda_i,$$

soit, en prenant $x \mapsto \exp(-x)$, qui est décroissante : $\frac{1}{n} \operatorname{tr} M \geq (\prod \lambda_i)^{1/n}$, ie

$$\det M \leq \left(\frac{\operatorname{tr} M}{n}\right)^n.$$

2. (a) Puisque M est définie positive, on a $M_{i,i} > 0$. On peut donc choisir $D_{i,i} = M_{i,i}^{-1/2}$.

(b) On a $D = {}^tD$. Calculons $\operatorname{Tr}({}^tDMD) = \sum (e_i|{}^tDMD e_i) = \sum_i (De_i|MD e_i) = \sum_i D_{i,i}^2 (e_i|Me_i) = n$.

(c) $DMD = {}^tDMD$ est symétrique et $\operatorname{tr} DMD \leq n$. Donc $\det M (\det D)^2 = \det DMD \leq 1$, d'où le résultat.

(d) $M = {}^tAA$ est une matrice symétrique positive et on obtient

$$(\det A)^2 = \det M \leq \prod_i \|A_i\|_2^2.$$

3. $\Phi: \mathbb{Q}_{m-1}[X] \times \mathbb{Q}_{n-1}[X] \rightarrow \mathbb{Q}^{n+m-1}[X]$
 $(P, Q) \mapsto PA + QB$

(a) Soit $D = \operatorname{pgcd}(A, B)$ unitaire dans $\mathbb{Q}[X]$. Les solutions de $AP + BQ = 0$ sont exactement $(P, Q) = \lambda(B/D, -A/D)$, où $\lambda \in \mathbb{Q}[X]$. On conclut en considérant les degrés.

(b) Φ est un isomorphisme si et seulement si $\operatorname{pgcd}(A, B) = 1$, donc s'il existe une unique solution (U, V) à $\Phi(U, V) = 1$.

(c) Dans la base $((X^{m-1}, 0), \dots, (1, 0), (0, X^{n-1}), \dots, (0, 1))$ au départ et $(X^{n+m-1}, \dots, 1)$ à l'arrivée, la matrice de Φ est la transposée de

$$M = \begin{pmatrix} a_n & a_{n-1} & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_n & \cdots & \cdots & a_0 & 0 & 0 & \\ \vdots & & \ddots & \ddots & & \ddots & \vdots & \\ & & & a_n & \cdots & & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_m & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots & \\ \vdots & & & \ddots & \ddots & & \ddots & \\ 0 & \cdots & \cdots & b_m & \cdots & \cdots & \cdots & b_0 \end{pmatrix}$$

On déduit alors, en considérant les lignes de M , que $\det M \leq \|A\|_2^m \cdot \|B\|_2^n$. Notez qu'il s'agit du résultat de A et B.

En utilisant les formules de Cramer, pour la résolution du système $\Phi(U, V) = (0, \dots, 0, 1)$, on obtient $U_i = \det M_i / \det M$, $i = 1, \dots, m$, où M_i est obtenu en remplaçant la i -ème colonne de M par $(0, \dots, 0, 1)$.

Mais alors $|\det M_i| \leq \|A\|_2^{m-1} \|B\|_2^n$.

Au final le dénominateur des coefficients de U et de V est majoré par $\det M = \|A\|_2^m \cdot \|B\|_2^n$, les numérateurs de ceux de U par $\|A\|_2^{m-1} \cdot \|B\|_2^n$ et ceux de V par $\|A\|_2^m \cdot \|B\|_2^{n-1}$.