TD DU 13/09/10 ET DU 20/09/10

Exercice 1.

On appelle entier algébrique tout nombre complexe x solution d'une équation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

où les a_i sont des entiers relatifs. On note $\mathbb{Z}[x]$ l'anneau engendré par x,

$$\mathbb{Z}[x] = \{y \in \mathbb{C} \mid y = P(x),\ P \in \mathbb{Z}[X]\}.$$

(1) Si $n = 2$ montrer que tout élément de $\mathbb{Z}[x]$ est un entier algébrique.
(2) Montrer plus généralement que, si $n \geqslant 3$, tout élément de $\mathbb{Z}[x]$ est un entier algébrique.

Exercice 2. Considérons la suite (u_n) définie comme suit :

$$u_0 = 4,\ u_1 = u_2 = 0,\ u_3 = 3,\ u_{n+4} = u_{n+1} + u_n.$$

(1) Écrire un programme Maple qui calcule les u_p pour p premier $\leqslant n$.
(2) Montrer que pour tout p premier, $p|u_p$.

---

1. Solutions

Solution 1

(1) Si $n = 2$ alors on a $x^2 = ax + b$ avec $(a, b) \in \mathbb{Z}^2$.
Soit $y \in \mathbb{Z}[x]$ et $Q = X^2 - aX - b$ alors $y = P(x)$ et si on divise P par le polynôme Q on obtient $P = QK + \alpha X + \beta$ d'où $y = P(x) = \alpha x + \beta$. Montrons que y est algébrique :

$$\begin{aligned} y^2 &= \alpha^2 x^2 + 2\alpha\beta x + \beta^2 = \alpha^2(ax + b) + 2\alpha\beta x + \beta^2 \\ &= \alpha x(\alpha a + 2\beta) + \alpha^2 b + \beta^2 = (y - \beta)(\alpha a + 2\beta) + \alpha^2 b + \beta^2 \end{aligned}$$

donc y est un entier algébrique.

(2) Là, il faut prendre les choses de plus haut sinon on va se noyer dans les calculs.

- Tout d'abord on pourra écrire $y = \sum\limits_{i=0}^{n-1} b_i x^i$ en divisant le polynôme P (dans $y = P(x)$) par le polynôme annulateur de x. Les b_i sont des entiers relatifs car le polynôme annulateur de x est unitaire.
- Plus généralement $yx^j = P(x)x^j$ va s'écrire $yx^j = \sum\limits_{i=0}^{n-1} c_{ij} x^i$ avec $c_{ij} \in \mathbb{Z}$.
- On réécrit cette dernière relation avec des matrices :
soit $X = (x^i)_{i \in [\![0,n-1]\!]}$ (matrice unicolonne) et $C = (c_{ij})_{(i,j) \in [\![0,n-1]\!]^2}$ alors les relations précédentes s'écrivent $yI_nX - CX = 0$ soit $(yI_n - C)X = 0$.
- Conclusion : la matrice $yI_n - C$ n'est pas inversible (car son noyau est non nul) donc $\det(yI_n - C) = 0$ or le développement de ce déterminant s'écrit

$$\begin{vmatrix} y - c_{00} & c_{01} & \cdots & c_{0\ n-1} \\ c_{10} & y - c_{11} & & \\ \vdots & & \ddots & \\ C_{n-1\ 0} & & & y - c_{n-1\ n-1} \end{vmatrix} = \prod_{i=0}^{n-1}(y - c_{ii}) + R(y)$$

où $R(y)$ est un polynôme de degré $\leqslant n - 1$ à coefficients entiers.
y est bien un entier algébrique.

Solution 2

(1)
```
u˜:=proc(n)
> local u,p,q,m;
> m˜:=prevprime(n);
> u[0]˜:=4;u[1]˜:=0;u[2]˜:=0;u[3]˜:=3;
> for p from 4 to m do u[p]˜:=u[p-3]+u[p-4] od;
> p˜:=2;
> while p <= m do
>   print(p,u[p],u[p]/p);
>   p˜:=nextprime(p);
> od;
> end;
```

(2) Que faire face à une telle suite, sinon calculer son,terme général ? Considérons le polynôme $P(X) = X^4 - X - 1$. Il est premier avec son polynôme dérivé (faire la division de P par P'. Comme les racines λ_i de P sont simples, u_n est une combinaison linéaire des λ_i^n. On a ainsi $u_n = \sum_{i=1}^{4} \alpha_i \lambda_i^n$ or $u_0 = 4 = \sum_{i=1}^{4} 1$, $u_1 = 0 = \sum_{i=1}^{4} \lambda_i$, $u_2 = 0 = \sum_{i=1}^{4} \lambda_i^2$ et, après un calcul simple, $u_3 = 3 = \sum_{i=1}^{4} \lambda_i^3$. Donc, comme on a un système de Cramer (Vandermonde), on peut conclure que $u_p = \lambda_1^p + \lambda_2^p + \lambda_3^p + \lambda_4^p$.
Or, $a^p + b^p = (a+b)^p - \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$, donc

$$u_p = (\lambda_1 + \lambda_2)^p + (\lambda_3 + \lambda_4)^p - \sum_{k=1}^{p-1} \binom{p}{k} (\lambda_1^k \lambda_2^{p-k} + \lambda_3^k \lambda_4^{p-k}).$$

Comme le coefficient de degré 3 est nul, la somme des racines est nulle, donc pour p premier et impair :

$$\begin{aligned} u_p &= -\sum_{k=1}^{p-1} \binom{p}{k} (\lambda_1^k \lambda_2^{p-k} + \lambda_3^k \lambda_4^{p-k}) \\ &= -\frac{1}{2} \sum_{k=1}^{p-1} \binom{p}{k} \left(\lambda_1^k \lambda_2^{p-k} + \lambda_1^{p-k} \lambda_2^k + \lambda_3^k \lambda_4^{p-k} + \lambda_3^{p-k} \lambda_4^k \right) \end{aligned}$$

(on a écrit deux fois l'expression de u_p en remplaçant k par $p-k$ dans la deuxième somme). Ce résultat est valable pour toute permutation de $\mathfrak{S}_4$, en particulier on aura le même calcul avec les regroupements (1,3) et (2,4), (1,4) et (2,3) ce qui fait que, en notant $S_{k,p-k} = \sum_{i \neq j} \lambda_i^k \lambda_j^{p-k}$ (tous les termes écrit dans cette somme sont distincts car $k \neq p-k$ et on a 12 termes en tout), on obtient

$$6u_p = -\sum_{k=1}^{p-1} \binom{p}{k} S_{k,p-k}.$$

Si on pose $S_k = \sum_{i=1}^{4} \lambda_i^k$ alors $S_k S_{p-k} = S_{k,p-k} + S_p$. On montre alors que $S_k \in \mathbb{Z}$ pour tout k, en effet, $\lambda_i^{4+k} = \lambda_i^{k+1} + \lambda_i^k$, on fait la somme et on récurre.
Pour p premier et $k \in [\![1, p-1]\!]$, $p | \binom{p}{k}$ donc $6u_p = pK$ où $K \in \mathbb{Z}$. $p | 6u_p$. On a vu que $p | u_p$ pour $p \in \{2, 3\}$ donc $p | u_p$ pour $p \geqslant 5$ premier.