

Algorithme d'Euclide étendu

Exercice 1

Soient A un anneau euclidien et a, b, c trois éléments de A . On suppose que a divise bc et que $\text{pgcd}(a, b) = 1$. Montrer que a divise c .

Exercice 2

Montrer que deux entiers impairs dont la différence est 32 sont premiers entre eux.

Exercice 3

Soit A un anneau intègre. Montrer que les propriétés suivantes sont équivalentes pour des éléments $a, b \in A$.

1. $\exists u \in A^\times$ tel que $a = ub$
2. $a|b$ et $b|a$
3. $(a) = (b)$

Pourriez-vous trouver un contre-exemple si A n'est pas supposé intègre? (On pourra essayer avec $A = \mathbb{Z}/10\mathbb{Z}$.)

Exercice 4

Existe-t-il $s, t \in \mathbb{Z}$ tels que $24s + 14t = 1$?

Exercice 5

Soient $a, b \in \mathbb{Z}$. Montrer que $(a) + (b) = (d)$ où $d = \text{pgcd}(a, b)$.

Exercice 6

Soit p un nombre premier. Dans chacun des cas suivants, calculer $\text{pgcd}(f, g)$ dans $\mathbb{F}_p[x]$ et une relation de Bezout à l'aide de l'algorithme d'Euclide étendu.

- (i) $f = x^3 + x + 1$, $g = x^2 + x + 1$, pour $p = 2$ et $p = 3$
- (ii) $f = x^4 + x^3 + x + 1$, $g = x^3 + x^2 + x + 1$, pour $p = 2$ et $p = 3$
- (iii) $f = x^5 + x^4 + x^3 + x + 1$, $g = x^4 + x^3 + x^2 + x + 1$ pour $p = 5$
- (iv) $f = x^5 + x^4 + x^3 - x^2 - x + 1$, $g = x^3 + x^2 + x + 1$, pour $p = 3$ et $p = 5$

Exercice 7

On définit la *norme* N sur l'anneau des entiers de Gauss $\mathbb{Z}[i]$ par $N(\alpha) = \alpha\bar{\alpha}$.

- 1) Montrer que N est une fonction euclidienne. (Indice : On pourra regarder le quotient $\frac{\alpha}{\beta}$ dans $\mathbb{C}$ de deux entiers de Gauss $\alpha, \beta \in \mathbb{Z}[i]$.)
- 2) Montrer que les inversibles de $\mathbb{Z}[i]$ sont exactement les éléments de norme 1, puis en dresser la liste.
- 3) Calculer tous les pgcd de 6 et $3 + i$ dans $\mathbb{Z}[i]$ ainsi que leurs représentations comme combinaisons linéaires de 6 et $3 + i$.
- 4) Calculer un pgcd de 12227 et $399 + 20i$.

Exercice 8

Soient F_n et F_{n+1} deux termes consécutifs de la suite de Fibonacci. Montrer qu'ils sont premiers entre eux.

Exercice 9

1) On note $(F_n)_{n \in \mathbb{N}}$ la suite de Fibonacci. Démontrer que

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right).$$

2) En déduire que le coût du calcul du pgcd de deux entiers de longueurs n et m est en $O(nm)$.

Exercice 10

1) Soit $a \in \mathbb{Z}$ fixé. Montrer que l'équation $42x + 18y = a$ admet une solution $(x, y) \in \mathbb{Z}^2$ si et seulement si a est un multiple de 6.

2) On suppose que a est multiple de 6. Soit (x_0, y_0) une solution particulière de l'équation précédente. Décrire l'ensemble des solutions.

3) Résoudre l'équation $6u + 10v + 15w = 1$ dans $\mathbb{Z}$.

Exercice 11

1) Calculer les solutions entières de l'équation diophantienne linéaire $24s + 33t = 9$.

2) Trouver tous les couples (f, g) de polynômes de $\mathbb{F}_3[x]$ satisfaisant l'équation

$$(x^2 + 1).f + (x + 2).g = x^2 + x + 1.$$

Exercice 12

Montrer que le polynôme $f = x^3 + x + 1$ est irréductible dans $\mathbb{F}_2[x]$. En déduire que l'anneau quotient $\mathbb{F}_2[x]/(f)$ est un corps. Combien a-t-il d'éléments ? Calculer les inverses de tous les éléments non nuls dans ce corps à l'aide de l'algorithme d'Euclide étendu.

Exercice 13

On considère les deux polynômes sur $\mathbb{Q}$ suivants :

$$f(X) = 6X^3 + 5X^2 + 9X + 8 \text{ et}$$

$$g(X) = 7X^2 - 10X + 2.$$

Calculer $\text{pgcd}(f, g)$ en utilisant l'algorithme d'Euclide étendu. Que remarquez vous ?

Exercice 14

On considère le corps $A = \mathbb{F}_7[x]/(x^3 + x + 1)$. Calculer l'inverse de la classe du polynôme $x + 3$ dans A .

Exercice 15

Soient $\mathbb{F}_q$ un corps fini à q éléments, $f \in \mathbb{F}_q[x]$ un polynôme de degré $n > 0$ et $A = \mathbb{F}_q[x]/(f)$ l'anneau quotient. On note $A^\times$ l'ensemble des éléments inversibles de l'anneau A . Alors $A^\times$ est un groupe multiplicatif. On note $\Phi(f)$ son cardinal. Si $g \in \mathbb{F}_q[x]$, on note $\overline{g}$ sa classe dans A .

1) Montrer que $\overline{g} \in A^\times$ si et seulement si f et g sont premiers entre eux.

2) Montrer que $\Phi(f) = q^n - 1$ si f est irréductible.

3) Montrer que $\Phi(f) = (q^d - 1)q^{n-d}$ si f est une puissance d'un polynôme irréductible de degré d .

Exercice 16

Trouver dans $\mathbb{Q}[x]$ les solutions du système de congruences

$$\begin{cases} P \equiv x + 1 \pmod{x^2 + x + 1} \\ P \equiv 3x + 2 \pmod{x^2 - x + 1}. \end{cases}$$

Approximants de Padé

Exercice 17

Faites la table de tous les approximants de Padé $(k, n - k)$ de $g = x^4 + x^3 + 3x^2 + 1 \in \mathbb{F}_5[x]$ pour $0 \leq k \leq n \leq 5$. Marquer les entrées de la table pour lesquelles il n'existe pas d'approximant.

Exercice 18

Donner tous les approximants de Padé dans $\mathbb{Q}(x)$ de la fonction exponentielle $\exp(x) = 1 + x + x^2/2 + x^3/6 + x^4/24 + \dots$ modulo x^5 .

Exercice 19

On considère le polynôme sur $\mathbb{Q}$ suivant :

$$f = \frac{1}{120}x^5 + \frac{1}{24}x^4 - \frac{1}{6}x^3 - \frac{1}{2}x^2 + x + 1.$$

Utiliser l'algorithme d'Euclide étendu pour calculer trois polynômes $U, V, G \in \mathbb{Q}[X]$ tels que

$$U \times X^6 + V \times f = G$$

et $\deg(G) \leq 3$ et $\deg(V) \leq 2$.

Le polynôme f est le développement limité de $\cos + \sin$ en 0 à l'ordre 6. Que peut on en déduire concernant la fraction rationnelle $\frac{G}{V}$?

Résultants

Exercice 20

On pose $f = x^4 - 3x^3 + 2x$ et $g = x^3 - 1$ dans $\mathbb{Q}[x]$. Calculer le pgcd h de f et g dans $\mathbb{Q}(x)$, puis dans $\mathbb{Z}[x]$. Vérifier que le résultant de f et g est nul, puis calculer $\text{res}(f/h, g/h)$. Calculer le pgcd de $\bar{f}$ et $\bar{g}$ dans $\mathbb{F}_3[x]$. Que constatez-vous ?

Exercice 21

Soient $f, g \in \mathbb{Z}[x]$ et p un nombre premier. On note h le pgcd de f et g et $\alpha = \text{lc}(h)$ son coefficient dominant. On suppose que p ne divise pas $\text{pgcd}(\text{lc}(f), \text{lc}(g))$ dans $\mathbb{Z}$. On dénote par une barre la réduction modulo p .

- 1) Montrer que α divise $\text{pgcd}(\text{lc}(f), \text{lc}(g))$.
- 2) Montrer que $\deg(\text{pgcd}(\bar{f}, \bar{g})) \geq \deg h$.
- 3) Montrer qu'il y a équivalence entre :

(a) $\deg(\text{pgcd}(\bar{f}, \bar{g})) = \deg h$

(b) $\bar{\alpha} \cdot \text{pgcd}(\bar{f}, \bar{g}) = \bar{h}$

(c) p ne divise pas $\text{res}(f/h, g/h)$ dans $\mathbb{Z}$.

À la lumière de cet exercice, expliquer le phénomène observé à l'exercice précédent.

Exercice 22

En utilisant les résultants, calculer un polynôme ayant pour racine $\sqrt{2} + \sqrt{3}$.

Exercice 23

Soit $P(x)$ un polynôme non constant à coefficients dans un corps, et dont les racines sont $\alpha_1, \dots, \alpha_n$.

- 1) Démontrer que le polynôme

$$R(y) = \text{Res}_x(P(x+y), P(-x))$$

admet pour racines les éléments $\alpha_i + \alpha_j$, $1 \leq i, j \leq n$.

- 2) On suppose en outre qu'aucune des racines de P n'est nulle. Démontrer que le polynôme $S(y) = \text{Res}_x(P(xy), P(x))$ admet pour racines les éléments α_i/α_j , $1 \leq i, j \leq n$.
- 3) Par analogie, déterminer une formule qui fournit un polynôme dont les racines sont les éléments $\alpha_i.\alpha_j$, $1 \leq i, j \leq n$.
- 4) Soient $K \subset L$ deux corps. En utilisant les résultats ci-dessus, montrer que l'ensemble des éléments de L qui sont algébriques sur K forment un sous-corps de L .

Exercice 24

On considère les deux courbes planes $X, Y \subset \mathbb{C}^2$ données par les polynômes

$$\begin{aligned}f(x, y) &= (y^2 + 6)(x - 1) - y(x^2 + 1) \\g(x, y) &= (x^2 + 6)(y - 1) - x(y^2 + 1)\end{aligned}$$

- 1) Calculer le résultant $\text{res}_y(f, g)$ de f et g relativement à la variable y .
- 2) En déduire la projection de $X \cap Y$ sur l'axe des x .
- 3) En déduire que $X \cap Y$ contient exactement 6 points dont on donnera les coordonnées.

Exercice 25

On considère les courbes planes

$$\begin{aligned}X &= \{(a, b) \in \mathbb{R}^2 \mid b - a^3 + 7a - 5 = 0\} \\Y &= \{(a, b) \in \mathbb{R}^2 \mid 20a^2 - 5ab - 4b^2 + 35a + 35b - 21 = 0\}\end{aligned}$$

dans $\mathbb{R}^2$. Déterminer l'intersection de X et Y de deux manières : en projetant sur la première coordonnée, puis en projetant sur la seconde coordonnée. Commenter les différences. Tracer les courbes et marquer leurs points d'intersection.

Exercice 26

- 1) Calculer le polynôme minimal $f \in \mathbb{Q}[x]$ de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$.
- 2) Soit $\mathbb{F}_{19^2} = \mathbb{F}_{19}[z]/(z^2 - 2)$ et $\alpha = \bar{z} \in \mathbb{F}_{19^2}$ une racine carrée de 2. Vérifier que 7α est une racine carrée de 3, et calculer le polynôme minimal de $\alpha + 7\alpha$ sur $\mathbb{F}_{19}$. Comment est-il relié à f ?

Exercice 27

Soit K un corps et soit $n \geq 2$ un entier.

- 1) Calculer le discriminant $\Delta(f) = \text{res}(f, f')$ d'un binôme $f = x^n + b$ avec $b \in K^\times$.
- 2) (Swann, 1962) Calculer le discriminant d'un trinôme $f = x^n + ax^k + b$ avec $1 \leq k < n$ et $a, b \in K^\times$.

Exercice 28

Soient ABC un triangle quelconque dont on note a, b, c les longueurs des cotés. Calculer l'aire du triangle ABC en fonction de a, b, c . On pourra introduire de nouvelles variables et utiliser les résultants.

Exercice 29

Soit $\mathcal{C}$ la courbe de $\mathbb{R}^2$ paramétrée par

$$\begin{cases} x(t) &= t^2 + t + 1 \\ y(t) &= \frac{t^2 - 1}{t^2 + 1} \end{cases}$$

où t parcourt $\mathbb{R}$.

- 1) Trouver un polynôme $P(X, Y) \in \mathbb{R}[X, Y]$ tel que pour tout point (x_0, y_0) de $\mathcal{C}$ on ait $P(x_0, y_0) = 0$. On justifiera rigoureusement que P convient. [Indication : Éliminer la variable t ...]