Anneaux euclidiens, division euclidienne, algorithme d'Euclide étendu

[STA] Structures Algébriques

19 octobre 2025

EPITA

Table des matières

$3x^2 + 5x + 1 \equiv 3.10^2 + 5.10^1 + 5.10^0$

Rappel : notion d'anneau euclidien

Les anneaux de polynômes

Anneaux quotients $\mathbb{R}$ $\sqrt{-1}$ i $i^2 = -1$ X $\boxed{X^2 = -1}$

Algorithme d'Euclide étendu et coefficients de Bézout

L'anneau des entiers de Gauss : $\mathbb{Z}[i]$

$a + ib$

$\in \mathbb{Z}$

Rappel : notion d'anneau euclidien

Définition : anneau euclidien

si $ab = 0$ alors $a = 0$ ou $b = 0$

Définition (Anneau euclidien)

Un **anneau euclidien** est un anneau intègre $(A, +, \cdot)$ muni d'un ***stathme***, c'est à dire une fonction

$$v : A^* \longrightarrow \mathbb{N}$$

telle que $\forall a \in A$, $\forall b \in A^*$, il existe $q, r \in A$ vérifiant :

$$\boxed{a = b \cdot q + r,} \quad \text{avec } \boxed{r = 0} \text{ ou } \boxed{v(r) < v(b).}$$

$b | a$

$\frac{p}{q} = xxxxx,xxx(yzt)^\infty$

Définition (Anneau euclidien)

Un **anneau euclidien** est un anneau intègre $(A, +, \cdot)$ muni d'un ***stathme***, c'est à dire une fonction

$$v : A^* \longrightarrow \mathbb{N}$$

telle que $\forall a \in A$, $\forall b \in A^*$, il existe $q, r \in A$ vérifiant :

$$a = b \cdot q + r, \quad \text{avec } r = 0 \text{ ou } v(r) < v(b).$$

Exemple

- $(\mathbb{Z}, +, \cdot)$ avec $v(n) = |n|$ $\in \mathbb{N}$
- $(\mathbb{Q}[X], +, \cdot)$ avec $v(P) = \deg(P)$ $\forall A \in \mathbb{Q}[X]\ \forall B \in \mathbb{Q}[X]\setminus\{0\}\ \exists Q, R\ \ A = B.Q + R$ où $\deg R < \deg Q$
- $(\mathbb{Z}[i], +, \cdot)$ avec $v(a + bi) = a^2 + b^2$

$\mathbb{Q}(i)$

$(a+bi)^{-1} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$

$z = a + ib$

$\bar{z} = a - ib$

$z^{-1} = \frac{\bar{z}}{|z|^2}$

$z\bar{z} = a^2 + b^2 = (a+ib)(a-ib) = (a)^2 - (ib)^2 = a^2 - (-b^2) = a^2 + b^2$

$A = 7x^{17}$

$B = 3x^3 + x$

$7x^{17} \mid 3x^3 + x$

$\hookrightarrow -\frac{7}{3}x^{15}$ $\quad \frac{7}{3}x^{14} - \frac{7}{9}x^{12}$

$\hookrightarrow \frac{7}{3}x^{13}$

$x^{13} \geq 3$

Exemple

Division euclidienne de 67 par 5.

$$
\begin{array}{rr|ll}
6 & 7 & 5 & \\ \cline{3-4}
-(5 & 0) & 1 & 0 \\ \hline
1 & 7 & & \\
-(1 & 5) & + & 3 \\ \hline
 & 2 & 1 & 3
\end{array}
$$

$$67 = 5 \cdot 13 + 2, \qquad q = 13,\ r = 2, \qquad v(r) = |2| = 2 < 5 = |5| = v(5)\,.$$

$$
\begin{array}{rr|l}
6 & 7 & 5 \\ \cline{3-3}
-(5 & 0) & 1\ 3 \\ \cline{1-2}
1 & 7 & \\
-(1 & 5) & \\ \cline{1-2}
(0 & 2) &
\end{array}
$$

$67 = 13 \times 5 + 2$

$|2| < |5|$

Q

Wooclap !

Exemple

On divise $A(X) = 3X^4 + 1X^3 + \frac{7}{2}X^2 + 2$ par $B(X) = 2X^2 + 1$.

$$
\begin{array}{rrrrr|lll}
3X^4 & +1X^3 & +\frac{7}{2}X^2 & +0X & +2 & 2X^2+1 & & \\
\hline
-(3X^4 & & \frac{3}{2}X^2 & &) & 3\cdot 2^{-1}X^2 & & \\
\hline
 & +1X^3 & +2X^2 & +0X & +2) & & & \\
 & -(1X^3 & & \frac{1}{2}X &) & & +1\cdot 2^{-1}X & \\
\hline
 & & 2X^2 & -\frac{1}{2}X & +2 & & & \\
 & & -(2X^2 & & +1) & & & +1 \\
\hline
 & & & -\frac{1}{2}X & +1 & \frac{3}{2}X^2 & +\frac{1}{2}X & +1
\end{array}
$$

$$A(X) = B(X)\cdot Q(X) + R(X), \qquad Q(X) = \frac{3}{2}X^2 + \frac{1}{2}X + 1,\ R(X) = -\frac{1}{2}X + 1,$$

$$v(R(X)) = \deg R(X) = 1 < 2 = \deg Q(X) = v(Q(X))\,.$$

$\frac{3}{2}x^2 \cdot (2x^2+1) = 3x^4 + \frac{3}{2}x^2$

$$
\begin{array}{rrrrr|l}
3x^4 & +1x^3 & +\frac{7}{2}x^2 & & +2 & 2x^2+1 \\
\hline
-(3x^4 & + & +\frac{3}{2}x^2) & & & \frac{3}{2}x^2 + \frac{1}{2}x + 1 \\
\hline
0 & +1x^3 & +\frac{4}{2}x^2 & & +2 & \\
-(& 1x^3 & + & \frac{1}{2}x) & & \\
\hline
 & 0 & +\frac{4}{2}x^2 & -\frac{1}{2}x & +2 & \\
 & -(& 2x^2 & & +1) & \\
\hline
 & & 0 & -\frac{1}{2}x & +1 &
\end{array}
$$

$\deg R < \deg 2x^2+1$

$$3x^4 + x^3 + \frac{7}{2}x^2 + 2 = (2x^2+1)\underbrace{\left(\frac{3}{2}x^2 + \frac{1}{2}x + 1\right)}_{Q} \underbrace{-\frac{1}{2}x + 1}_{R}$$

$4 = \{4 + k5 : k \in \mathbb{Z}\}$

$4 = 9 \mod 5$

$\boxed{4} \times 3 = 12 = 2 \mod 5$

$\boxed{9} \times (-2)$
$= -18$
$= -4 \times 5 + 2 \pmod 5$

$\mathbb{Z}/3\mathbb{Z}$ un corps

premier $\Rightarrow$

$0 \rightarrow$ pas d'inverse

$1^{-1} \rightarrow 1$

$2 \rightarrow u$ tq $2 \times u = 1 \mod 5 \quad = 2$

$2 \times 3 = 6 = 5 + 1 = 1 \mod 5$

$5 = 0$

$(-18) \times 3 = -54$
$= -4$
$= 1 \mod 5$

$2 = -18$

Wooclap !

$3 = 2^{-1}$ "$3 = 1/2$" $\mod 5$

$3 \rightarrow 3 \times 2 = 1 \mod 5$
$\rightarrow 3^{-1} = 2$

x:	0	1	2	3	4
x^{-1}:	$\times$	1	3	2	4

$4 \times 4 = 16 = 3 \times 5 + 1 = 1 \mod 5$

$\frac{3}{4} = 3 \times 4 = 12$
$= 3 \times \frac{1}{4}$
$= 4$
$= -3$
$= 2 \mod 5$

$4x = 1 = 4y$

$4 \cdot (x - y) = 0$

$\frac{8}{3} = \frac{3}{3} = 1$

$8 \times 2 = 16 = 2$

$\frac{1}{3} - \frac{4}{2} = 2 - \frac{4}{2} = 0$
$= 2$
$\frac{7}{2} - \frac{12}{2} = -\frac{5}{2} = 0$

$$
\begin{array}{l|l}
3x^4 + x^3 \qquad + 1 & 2x^2 + 3 \\
-(3x^4 \qquad + 2x^2) & 4x^2 + 3x + \frac{3}{2} \\
\hline
0 + x^3 - 2x^2 + 1 & \\
-(6x^3 \qquad + 9x) & \\
\hline
0 + 3x^2 + x + 1 & \\
-(3x^2 \qquad + \frac{9}{2}) & \\
\hline
0 + x - \frac{7}{2} &
\end{array}
$$

$9 \times 3 = 27 = 2 \mod 5$

$0 + x - \frac{7}{2} = x - \frac{2}{2} = x - 1 = x + 4$

$3 \times \frac{1}{2} = 3 \times 2^{-1}$
$= 3 \times 3$
$= 9$
$= 4$

$\left(\frac{2}{3}\right)^{-1} = \frac{3}{2}$
$= 3 \times 3$
$= 9$
$= 4$

$(2 \times 2)^{-1} = 4$

Les anneaux de polynômes

L'anneau $(A[X], +, \cdot)$

Définition

Soit $(A, +, \cdot)$ un anneau. On note $(A[X], +, \cdot)$ l'anneau des polynômes à coefficients en A avec les l'addition et la multiplication de polynômes classiques [a].

On a $P(X) \in A[X] \Leftrightarrow P(X) = 0$ ou $\exists n \in \mathbb{N},\ \exists (a_i)_{i=0}^{n} \in A, a_n \neq 0,$

$$P(X) = \sum_{k=0}^{n} a_k X^k = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n .$$

a. La formulation formelle de l'anneau et ses opérations est lourde. Si vous êtes motivés, écrivez-la et montrez-la moi pour validation.

Exemple

- $(\mathbb{Z}[X], +, \cdot)$: polynômes à coefficients entiers. pas euclidien $2x + x$
- $(\mathbb{Q}[X], +, \cdot)$: polynômes à coefficients rationnels. euclidien
- $(\mathbb{Z}/n\mathbb{Z}[X], +, \cdot)$: polynômes à coefficients dans $\mathbb{Z}/n\mathbb{Z}$. euclidien qd n est 1er

si n n'est pas 1er $n = p \times q$ $(pX)(qX) = \underbrace{(pq)}_{=0}X^2 = 0$ pas intègre

Degré d'un polynôme

Définition (Degré d'un polynôme)

Soit $P(X) \in A[X]$.

- Si $\exists n \in \mathbb{N}, \exists (a_i)_{i=0}^{n} \in A, a_n \neq 0$, alors on a $\deg(P(X)) = n$
- Si $P(X) = 0$, on pose $\deg(P(X)) = \boxed{\deg(0) = -\infty}$

deg A+B = dgA + dgB

$-\infty + A = -\infty$

Proposition

Soit $(A, +, \cdot)$ un domaine d'intégrité. Soient $P(X), Q(X) \in A[X]$. Alors,

$$\boxed{\deg(P(X) \cdot Q(X)) = \deg(P(X)) + \deg(Q(X))\,.}$$

Démonstration.

Fastidieuse. On traite d'abord les cas particuliers où P ou Q sont 0. Ensuite, on déduit que si $(a_i)_{i=0}^{n}$ et $(b_j)_{j=0}^{m}$ sont les coefficients de P et Q, on a $\boxed{a_n \cdot b_m} \neq 0$ grâce à la propriété d'intégrité de A. □

deg des mono $\neq$ nul $\in \{0, \dots, n+m\}$

ms

Question

Propriétés d'anneaux de polynômes

$[i)\ AB = \sum_{k=0}^{i} a_i b_{k-i} = \sum_{k=0}^{i} b_{k-i} a_i = \sum_{k=0}^{i} b_i a_{k-i} = [i)\ BA$

$A[X]$ comm $\Rightarrow \underbrace{(aX)(bX)}_{(ab)X^2} = (bX)(aX)$

$(ab)X^2 = (ba)X^2 \Rightarrow ab = ba$

$\Rightarrow A$ est comm.

Question

1. À quelle condition est-ce que $(A[X], +, \cdot)$ est commutatif ?

$[i]P$ = le coeff de X^i dans le polynôme P

Question

1. À quelle condition est-ce que $(A[X], +, \cdot)$ est commutatif ?
2. À quelle condition est-ce que $(A[X], +, \cdot)$ est intègre ?

constants

si A[X] intègre : A(X) contient les polynômes cts donc si A[X] est intègre

or $\forall a, b$ $a \times b = 0$
$\Rightarrow a = 0$
ou $b = 0$

$\Rightarrow$ A est intègre

si A est intègre le coeff dom de $\overset{\neq 0}{A} \times \overset{\neq 0}{B}$ le prod des coefs dominants de A et de B qui est $\neq 0$ donc A[X] est intègre

$\forall A, B, (A \times B = 0 \Rightarrow A = 0$ ou $B = 0)$

$\Leftrightarrow \forall A, B$ $(A \neq 0$ et $B \neq 0 \Rightarrow A \times B \neq 0)$

$\Phi \Rightarrow \Psi$

non $\Psi \Rightarrow$ non Φ

Question

1. À quelle condition est-ce que $(A[X], +, \cdot)$ est commutatif ?
2. À quelle condition est-ce que $(A[X], +, \cdot)$ est intègre ?
3. À quelle condition est-ce que $(A[X], +, \cdot)$ est euclidien ? A est un corps

on doit pouvoir diviser X par aX pour tout $a \neq 0$ dans A

$$X = aX \cdot Q + R \quad \deg R < \deg(aX)$$

$\deg 0$, cte

$Q = b$

$= b = a^{-1}$

Propriétés d'anneaux de polynômes

Question

1. À quelle condition est-ce que $(A[X], +, \cdot)$ est commutatif ?
2. À quelle condition est-ce que $(A[X], +, \cdot)$ est intègre ?
3. À quelle condition est-ce que $(A[X], +, \cdot)$ est euclidien ? A est corps
4. À quelle condition est-ce que $(A[X], +, \cdot)$ est un corps ? jamais X n'a pas d'inv.

$\deg X \cdot A = \deg X + \deg A \geqslant 1 > 0$

$X \cdot A = 1$

$\Downarrow$ polynome cte $\Rightarrow$ A est un corps

Anneaux quotients

Disclaimer

La définition d'anneau quotien demande l'introduction de la notion d'*idéal*. Étant donné que cela demande un niveau d'abstraction (encore) plus important, nous allons voir une version simplifié de cette notion : le quotient d'un anneau par (l'idéal généré par) un élément, et, plus particulièrement, le cas où l'anneau est un domaine euclidien.

Quotient d'un domaine euclidien

$\mathbb{Z}/n\mathbb{Z}$ $= \mathbb{Z}/(n)$ $\mathbb{Z}/n\mathbb{Z}$ $A = B(x^3+7) + R$ $\deg < 3$

Définition (Anneau quotient)

Soit $(A, +, \cdot)$ un domaine euclidien. Soit $a \in A$. On appelle **anneau quotient** de A par (a) à l'anneau $(A/(a), +, \cdot)$ où $A/(a)$ est l'ensemble des classes d'équivalence de la relation

$$x \sim y \Leftrightarrow a \mid x - y \Leftrightarrow \exists k \in A, a \cdot k = x - y$$

On note une classe d'équivalence $[x]$. Les opérations sont : $\forall x, y \in A$,

$\to \mathbb{Z}/5\mathbb{Z} = \mathbb{Z}/(5)$

$$[x] + [y] = [x + y] \qquad [x] \cdot [y] = [x \cdot y]$$

$\mathbb{Z}[X]/(x^3+7)$

$\mathbb{Z}_5/\mathbb{Z}[X]/x^{17}+2$

$x^4 - (-7x) = x^4 + 7x$

$= x(x^3+7)$

$=$ multiple de x^3+7

$x^4 = x(x^3)$

$= x(x^3 + 7 - 7)$

$= x(x^3+7) - 7x$

$= -7x \mod (x^3+7)$

Quotient d'un domaine euclidien

Définition (Anneau quotient)

Soit $(A, +, \cdot)$ un domaine euclidien. Soit $a \in A$. On appelle **anneau quotient** de A par (a) à l'anneau $(A/(a), +, \cdot)$ où $A/(a)$ est l'ensemble des classes d'équivalence de la relation

$$x \sim y \Leftrightarrow a \mid x - y \Leftrightarrow \exists k \in A, a \cdot k = x - y$$

On note une classe d'équivalence $[x]$. Les opérations sont : $\forall x, y \in A$,

$$[x] + [y] = [x + y] \qquad [x] \cdot [y] = [x \cdot y]$$

Proposition

Si A est un domaine euclidien, alors

$$[x] = [r_x]$$

où r_x est le reste de la division euclidienne de x par a.

$x^4 = x(x^3+7) - 7x$

$[x^4] = [-7x]$

$\mathrm{mod}\ (x^3+7)$

$x = q\,a + r_x$

$= r_x \ \mathrm{mod}\ a$

Exemples

Les deux exemples qu'on va utiliser sont :

Exemples

Les deux exemples qu'on va utiliser sont :

Exemple

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n)$

C'est le cas qui inspire cette construction.

Les deux exemples qu'on va utiliser sont :

Exemple

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n)$

C'est le cas qui inspire cette construction.

Exemple

Soit $P(X) \in A[X]$. On peut définir $A[X]/(P(X))$.

$\mathbb{C} \equiv \mathbb{R}[X]/X^2+1$

$a+ib \equiv a+bX$

$(a+ib)(c+id) = \underline{ac-bd} + i\underline{(ad+bc)}$

$(a+Xb)(c+Xd) = ac + X(bc+ad) + X^2 db$

$= ac + X(bc+ad) - bd$

$= \underline{(ac-bd)} + X\underline{(bc+ad)}$

$\boxed{X^2 = (X^2+1) - 1 = -1}$

Exemple : $\mathbb{Q}[X]/(X^2-1)$

Exemple

Considérons l'anneau quotient

$$\underbrace{A = \mathbb{Q}[X]/(X^2-1).}$$

$X^2 - 1 = 0 \quad X^2 = 1$

Exemple : $\mathbb{Q}[X]/(X^2-1)$

Exemple

Considérons l'anneau quotient

$$A = \mathbb{Q}[X]/(X^2-1).$$

$$X^2 = 1 = \underbrace{(X^2-1)}_{=0} + 1$$

Tout élément de A s'écrit de manière unique (***pourquoi ?***) de la forme

$$[a+bX], \quad a, b \in \mathbb{Q}.$$

$$X^{17} = X^{2\times 8+1} = (\underbrace{X^2}_{=1})^8 \cdot X = X$$

$$X^{2k+1} = X$$

$$X^{2k} = 1$$

$$5X^{23} + 3X^{17} + 42X^6 = 8X + 42$$

$[A] = [r_A]$ où r_A est le reste de la division euclidienne de A par X^2-1

$$\deg r_A < \deg(X^2-1) = 2$$

donc $\forall A, \exists a, b$ tq $[A] = [a+bX]$ où a et b sont les coefs de r_A

Prouvons l'unicité :

si $[a+bX] = [c+dX]$

$$\underbrace{(a+bX) - (c+dX)}_{\deg \leq 1} \underset{\text{vrai } =}{=} \text{multiple de } \underbrace{(X^2-1)}_{\deg 2}$$

le seul multiple de X^2-1 qui soit de $\deg \leq 1$ est 0

donc

$$(a+bX) - (c+dX) \underset{\text{vrai } =}{=} 0 \text{ donc } \boxed{a = c \text{ et } b = d}$$

Exemple : $\mathbb{Q}[X]/(X^2-1)$

Exemple

Considérons l'anneau quotient

$$A = \mathbb{Q}[X]/(X^2-1).$$

Tout élément de A s'écrit de manière unique (***pourquoi ?***) de la forme

$$[a+bX], \quad a, b \in \mathbb{Q}\,.$$

Regardons deux éléments particuliers :

$$[X-1] \neq [0], \quad [X+1] \neq [0], \qquad \text{et} \qquad [X-1]\cdot[X+1] = [X^2-1] = [0].$$

$(x-1)(x+1) = x^2-1 = 0$ pas intègre

Exemple : $\mathbb{Q}[X]/(X^2 - 1)$

Exemple

Considérons l'anneau quotient

$$A = \mathbb{Q}[X]/(X^2 - 1).$$

Tout élément de A s'écrit de manière unique (***pourquoi ?***) de la forme

$$[a + bX], \quad a, b \in \mathbb{Q}.$$

Regardons deux éléments particuliers :

$$[X - 1] \neq [0], \quad [X + 1] \neq [0], \qquad \text{et} \qquad [X - 1] \cdot [X + 1] = [X^2 - 1] = [0].$$

Donc l'anneau $A = \mathbb{Q}[X]/(X^2 - 1)$ contient des **diviseurs de zéro** : c'est donc un anneau **non intègre**.

Exemple

Considérons maintenant l'anneau quotient

X "$=$ i"

$$A = \mathbb{R}[X]/(X^2+1).$$

Exemple : $\mathbb{R}[X]/(X^2+1)$

Exemple

Considérons maintenant l'anneau quotient

$$A = \mathbb{R}[X]/(X^2+1).$$

Tout élément de A peut s'écrire sous la forme $[a+bX], \quad a, b \in \mathbb{R}$. et on a

Exemple : $\mathbb{R}[X]/(X^2+1)$

Exemple

Considérons maintenant l'anneau quotient

$$A = \mathbb{R}[X]/(X^2+1).$$

Tout élément de A peut s'écrire sous la forme $[a+bX], \quad a, b \in \mathbb{R}$. et on a

$$[X^2+1] = [0] \Rightarrow [X \cdot X] + [1] = [0] \Rightarrow [X]^2 = -[1]$$

Exemple : $\mathbb{R}[X]/(X^2+1)$

X^2+3

Exemple

Considérons maintenant l'anneau quotient

$$A = \mathbb{R}[X]/(X^2+1).$$

Tout élément de A peut s'écrire sous la forme $[a+bX], \quad a, b \in \mathbb{R}$. et on a

$$[X^2+1] = [0] \Rightarrow [X \cdot X] + [1] = [0] \Rightarrow [X]^2 = -[1]$$

Les opérations s'écrivent

$$[a+bX] + [c+dX] = [(a+c) + (b+d)X]$$
$$[a+bX] \cdot [c+dX] = [ac + (ad+bc)X + bdX^2] = [(ac-bd) + (ad+bc)X]$$

$K \to K[X]$ euclidien $\to K[X]/P$ si P est bien choisi, c'est un corps + grand

corps à 25 elts

Exemple : $\mathbb{R}[X]/(X^2+1)$

Quels sont les carrés de $\mathbb{Z}_5$?

x	0	1	2	3	4
x^2	0	1	4	4	1

$(x^2+2 \neq 0\ \forall x \in \mathbb{Z}_5)$ X^2-3 n'a pas de sol dans $\mathbb{Z}_5$

$\mathbb{Z}_5 \to \mathbb{Z}_5[X] \to \mathbb{Z}_5[X]/_{X^2+2}$

$\mathbb{R} \to \mathbb{R}[X] \to \mathbb{R}[X]/_{X^2+1} \to \mathbb{C}$

Exemple

Considérons maintenant l'anneau quotient

$$A = \mathbb{R}[X]/(X^2+1).$$

Tout élément de A peut s'écrire sous la forme $[a+bX]$, $\quad a, b \in \mathbb{R}$. et on a

$$[X^2+1] = [0] \Rightarrow [X \cdot X] + [1] = [0] \Rightarrow [X]^2 = -[1]$$

Les opérations s'écrivent

$$[a+bX] + [c+dX] = [(a+c) + (b+d)X]$$

$$[a+bX] \cdot [c+dX] = [ac + (ad+bc)X + bdX^2] = [(ac-bd) + (ad+bc)X]$$

Question

Ça vous rappelle quelque chose ?

$\mathbb{C}$

$$(a+xb) \cdot \frac{(a-xb)}{a^2+b^2} = 1$$

$a x^{17} \ldots$

$$\begin{array}{l|l} & b x^3 \\ \hline & \frac{a}{b} x^{14} \end{array}$$

Algorithme d'Euclide étendu et coefficients de Bézout

A anneau

$A/a \quad a \in A$

$A = \mathbb{Z}$, $a = n$, $A/a = \mathbb{Z}/n\mathbb{Z}$

$A = \mathbb{R}[X]$, $a = X^2+1$, $A/a = \mathbb{R}[X]/X^2+1$

Bezout : si $x \in A$ tq $a \wedge x = 1$ alors $\exists\, u, v \in A$ tq ← $\exists$ algo

$au + xv = 1$

algorithme qui permet de trouver l'inverse de $x \in A/a$ s'il existe

$\Rightarrow xv = 1 - \underbrace{au}_{\text{multiple de } a} = 1$ modulo a

$\Rightarrow v = x^{-1}$ ds A/a

Idée clé

Pour $a, b \in A$ (anneau euclidien), on effectue des divisions successives :

$a = 0 \cdot (a+1) + a \leftarrow r_{-1} = a$

$b = a \cdot 0 + b \leftarrow r_0 = b$

$$\begin{cases} a = b \cdot q_1 + r_1, & \to r_1 = a \cdot 1 - b \cdot q_1 = \\ b = r_1 \cdot q_2 + r_2, & \to r_2 = b \cdot 1 - r_1 \cdot q_2 \\ r_1 = r_2 \cdot q_3 + r_3 & \to r_3 = r_1 - r_2 \cdot q_3 \\ \vdots \\ r_{n-2} = r_{n-1} \cdot q_n + r_n, \\ r_{n-1} = r_n \cdot q_{n+1} + \underset{r_{n+1}}{0} \end{cases}$$

Le dernier reste non nul r_n est le **PGCD** de a et b.

On cherche $(u_i$ et v_i tq $\boxed{\forall i \quad r_i = a \cdot u_i + b \cdot v_i}$

$r_{-1} = a = a \cdot 1 + b \cdot 0 \to u_{-1} = 1 \; v_{-1} = 0$

$r_0 = b = a \cdot 0 + b \cdot 1 \to u_0 = 0, v_0 = 1$

pgcd $r_n = a \cdot \underset{u}{u_n} + b \cdot \underset{v}{v_n}$

$r_{i-2} = r_{i-1} \cdot q_i + r_i \to r_i = r_{i-2} - q_i \, r_{i-1}$

$= (a \, u_{i-2} + b \cdot v_{i-2}) - q_i (a \, u_{i-1} + b \, v_{i-1})$

$= a \, u_i + b \, v_i$

$$\Rightarrow \boxed{\forall i \quad \begin{cases} u_i = u_{i-2} - q_i \, u_{i-1} \\ v_i = v_{i-2} - q_i \, v_{i-1} \end{cases}}$$

$\in A$

$$\boxed{\text{C.I.} : \begin{cases} u_{-1}, v_{-1} = 1, 0 \\ u_0, v_0 = 0, 1 \end{cases}}$$

$$\begin{pmatrix} u_{i-1} \\ u_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} u_{i-2} \\ u_{i-1} \end{pmatrix}$$

$u_{i-1} = 0 \cdot u_{i-2} + 1 \cdot u_{i-1}$

$u_i = u_{i-2} \cdot 1 - q_i \, u_{i-1}$

$$\begin{pmatrix} v_{i-1} \\ v_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} v_{i-2} \\ v_{i-1} \end{pmatrix}$$

Principe de l'algorithme d'Euclide

Idée clé

Pour $a, b \in A$ (anneau euclidien), on effectue des divisions successives :

$$\begin{cases} a = b \cdot q_1 + r_1, \\ b = r_1 \cdot q_2 + r_2, \\ \quad \vdots \\ r_{n-2} = r_{n-1} \cdot q_n + r_n, \\ r_{n-1} = r_n \cdot q_{n+1}. \end{cases}$$

Le dernier reste non nul r_n est le **PGCD** de a et b.

Version étendue

On exprime à chaque étape $r_k = a \cdot u_k + b \cdot v_k$: les coefficients (u_k, v_k) sont les **coefficients de Bézout**.

Exemple détaillé en $\mathbb{Z}$: $(a, b) = (56, 15)$

$r_i = a \cdot u_i + b \cdot v_i$

$u_i = u_{i-2} - q_i \cdot u_{i-1}$

i	u_i	v_i
-1	1	0
0	0	1
1	1	-3
2	-1	4
3	3	-11
4	-4	15

$u_1 = u_{-1} - q_1 \cdot u_0$

$1 - 3 \cdot 0 = 2$

$r_3 = 3 = 3 \times 56 - 11 \times 15$

$r_2 = 4 = a \times -1 + b \times 4$

$= -56 + 15 \times 4 = 4$

56, 15

(1) $56 = 3 \cdot 15 + 11$

(2) $15 = 1 \cdot 11 + 4$

(3) $11 = 2 \cdot 4 + 3$

(4) $4 = 1 \cdot 3 + 1$

$r_4 = 1$

Exemple
Divisions

$$56 = 3 \cdot 15 + 11 \Rightarrow 11 = 56 - 3 \cdot 15$$
$$15 = 1 \cdot 11 + 4 \Rightarrow 4 = 15 - 1 \cdot 11$$
$$11 = 2 \cdot 4 + 3 \Rightarrow 3 = 11 - 2 \cdot 4$$
$$4 = 1 \cdot 3 + 1 \Rightarrow 1 = 4 - 1 \cdot 3$$

$3 = 1 \cdot 3 + 0$

$r_4 = r_3 - q_4 \cdot r_2$

Ainsi $\mathrm{PGCD}(56, 15) = 1$.

$15 \times 15 = 225$

$56 \times 4 = 224$

$r_4 = 1 = a \times -4 + b \times 15$

$\mathrm{inv} = g = a\, u_k + b\, v_k$

$u = u_k \cdot g^{-1}$

A B

$A = B \cdot Q_1 + R_1$ $\qquad \deg R < \deg B$

si $R_1 \neq 0$: $B = R_1 \cdot Q_2 + R_2$ $\qquad \deg R_2 < \deg R_1$ $\qquad \forall i$: $\deg R_i < \deg R_{i-1}$

si $R_2 \neq 0$: $R_1 = R_2 \cdot Q_3 + R_3$ $\qquad \deg R_3 < \deg R_2$

do $\mathbb{Z}_4$

$2 \cdot 0 = 0$

$2 \cdot 1 = 2$

$2 \cdot 2 = 4 = 0$

$2 \cdot 3 = 6 = 2$

Exemple détaillé en $\mathbb{Z}$: $(a, b) = (56, 15)$

Exemple

Divisions

$$\begin{aligned} 56 &= 3\cdot 15 + 11 &\Rightarrow\quad 11 &= 56 - 3\cdot 15 \\ 15 &= 1\cdot 11 + 4 &\Rightarrow\quad 4 &= 15 - 1\cdot 11 \\ 11 &= 2\cdot 4 + 3 &\Rightarrow\quad 3 &= 11 - 2\cdot 4 \\ 4 &= 1\cdot 3 + 1 &\Rightarrow\quad 1 &= 4 - 1\cdot 3 \end{aligned}$$

Ainsi $\mathrm{PGCD}(56, 15) = 1$.

Substitutions

$$\begin{aligned} 1 &= 4 - 1\cdot 3 \\ &= 4 - (11 - 2\cdot 4) = 3\cdot 4 - 1\cdot 11 \\ &= 3(15 - 1\cdot 11) - 1\cdot 11 = 3\cdot 15 - 4\cdot 11 \\ &= 3\cdot 15 - 4(56 - 3\cdot 15) \\ &= 15\cdot 15 - 4\cdot 56 \end{aligned}$$

Exemple détaillé en $\mathbb{Z}$: $(a,b) = (56,15)$

Exemple

Divisions

$$\begin{aligned} 56 &= 3\cdot 15 + 11 &\Rightarrow\quad 11 &= 56 - 3\cdot 15 \\ 15 &= 1\cdot 11 + 4 &\Rightarrow\quad 4 &= 15 - 1\cdot 11 \\ 11 &= 2\cdot 4 + 3 &\Rightarrow\quad 3 &= 11 - 2\cdot 4 \\ 4 &= 1\cdot 3 + 1 &\Rightarrow\quad 1 &= 4 - 1\cdot 3 \end{aligned}$$

Ainsi $\mathrm{PGCD}(56,15) = 1$.

Substitutions

$$\begin{aligned} 1 &= 4 - 1\cdot 3 \\ &= 4 - (11 - 2\cdot 4) = 3\cdot 4 - 1\cdot 11 \\ &= 3(15 - 1\cdot 11) - 1\cdot 11 = 3\cdot 15 - 4\cdot 11 \\ &= 3\cdot 15 - 4(56 - 3\cdot 15) \\ &= 15\cdot 15 - 4\cdot 56 \end{aligned}$$

$$\boxed{1 = (-4)\cdot 56 + 15\cdot 15} \quad\Rightarrow\quad \boxed{u = -4,\ v = 15}$$

Problème

Étant donné un nombre premier p et un élément $[a] \in \mathbb{Z}/p\mathbb{Z}$, on cherche son **inverse modulaire** $[a]^{-1}$, c'est à dire l'élément tel que :

$$[a] \cdot [a]^{-1} = [1] .$$

Inverse modulaire dans un corps fini $\mathbb{Z}/p\mathbb{Z}$

Problème

Étant donné un nombre premier p et un élément $[a] \in \mathbb{Z}/p\mathbb{Z}$, on cherche son **inverse modulaire** $[a]^{-1}$, c'est à dire l'élément tel que :

$$[a] \cdot [a]^{-1} = [1] .$$

Condition d'existence : L'élément $[a]$ est inversible si et seulement si $\mathrm{PGCD}(a, p) = 1$. C'est toujours vrai si p est premier et $[a] \neq [0]$.

Inverse modulaire dans un corps fini $\mathbb{Z}/p\mathbb{Z}$

Problème

Étant donné un nombre premier p et un élément $[a] \in \mathbb{Z}/p\mathbb{Z}$, on cherche son **inverse modulaire** $[a]^{-1}$, c'est à dire l'élément tel que :

$$[a] \cdot [a]^{-1} = [1] \,.$$

Condition d'existence : L'élément $[a]$ est inversible si et seulement si $\mathrm{PGCD}(a, p) = 1$. C'est toujours vrai si p est premier et $[a] \neq [0]$.

Principe : algorithme d'Euclide étendu et calcul des coefficients de Bézout.

$$\boxed{1 = u \cdot p + v \cdot a.}$$

En passant à la congruence modulo p :

$$[1] = [u \cdot p + v \cdot a] = [u] \cdot [p] + [v] \cdot [a] \overset{[p]=[0]}{=} [v] \cdot [a].$$

Ainsi :

$$[a]^{-1} = [v].$$

$1 = (-3.10) - 2.(4.10)$ $\quad$ $3 = 4.10 \bmod 37$ $\quad$ $7 = -3.10 \bmod 37$

$\leftarrow 3 = 10 - (-3.10) \bmod 37$

Bezout

10 ds $\mathbb{Z}/37\mathbb{Z}$

$$\boxed{10 . u = 1 \bmod 37}$$

$$\boxed{10 . u = 1 + 37 v}$$

$\in \mathbb{Z}$ $\quad$ $\in \mathbb{Z}$

↳ 10 et 37 sont premiers entre eux ds $\mathbb{Z}$

$$37 = 3.10 + 7$$
$$10 = 1.7 + 3$$
$$7 = 2.3 + 1$$
$$3 = 3.1 + 0$$

$$7 = \underbrace{\cancel{37}.1} - \underbrace{3.10}$$
$$3 = \underbrace{10 - 1.7}$$
$$\rightarrow 1 = 7 - \underbrace{2.3}$$

$$3 = 10.1 - 1.(\cancel{37}.1 - 3.10)$$
$$3 = 4.10 - \cancel{37}$$

Wooclap !

10×26

$$\begin{array}{r|l} 260 & 37 \\ \cline{2-2} -259 & 7 \\ \hline 1 & \end{array}$$

$7 \times 37 = \underline{259}$

$$1 = 7 - 2.3$$
$$= \cancel{37}.1 - 3.10 - 2[4.10 - \cancel{37}]$$
$$= -11.10 + x.\cancel{37}$$
$$3 \times 37$$
$$= 26.10$$

L'anneau des entiers de Gauss :

$\mathbb{Z}[i]$

Définition de $\mathbb{Z}[i]$

$$\mathbb{Z}[i] \simeq \mathbb{Z}[X]/_{X^2+1}$$

Définition

L'anneau des **entiers de Gauss** est : $i \in \mathbb{C}$

$$\mathbb{Z}[i] = \{\, a + bi \mid a, b \in \mathbb{Z} \,\},$$

avec les opérations usuelles :

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \quad (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Définition de $\mathbb{Z}[i]$

Définition

L'anneau des **entiers de Gauss** est :

$$\mathbb{Z}[i] = \{\, a + bi \mid a, b \in \mathbb{Z} \,\},$$

avec les opérations usuelles :

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \quad (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Stathm euclidien

On définit $v(a + bi) = a^2 + b^2$.

$(a+ib)(a-ib) = a^2+b^2$

Comment on réalise la division euclidienne ?

Idée de l'algorithme dans $\mathbb{Z}[i]$

Soient $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. On cherche $q, r \in \mathbb{Z}[i]$ tels que

$$a = b \cdot q + r, \qquad v(r) < v(b).$$

Comment on réalise la division euclidienne ?

Idée de l'algorithme dans $\mathbb{Z}[i]$

Soient $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. On cherche $q, r \in \mathbb{Z}[i]$ tels que

$$a = b \cdot q + r, \qquad v(r) < v(b).$$

Procédure :

1. On calcule le quotient complexe $\frac{a}{b} = x + iy \in \mathbb{C}$.
2. On arrondit séparément les parties réelles et imaginaires pour obtenir un élément de $\mathbb{Z}[i]$: $q = \lfloor x \rceil + i \lfloor y \rceil$
3. On calcule le reste $r = a - b \cdot q$.
4. Par construction [a], $v(r) \leq \frac{1}{2} v(b) < v(b)$.

Comment on réalise la division euclidienne ?

$a = u + iv$, $b = z + iw$

$$\frac{a}{b} = \overbrace{(u+iv)\cdot\frac{z-iw}{z^2+w^2}}^{= x+iy}$$

dans $\mathbb{C}$

Idée de l'algorithme dans $\mathbb{Z}[i]$

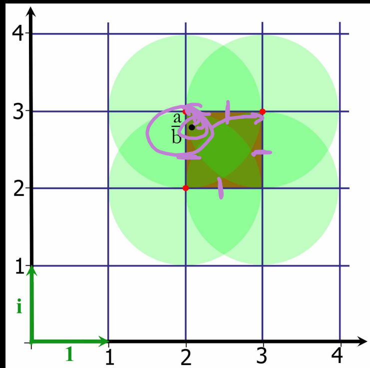
Soient $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. On cherche $q, r \in \mathbb{Z}[i]$ tels que

$$a = b \cdot q + r, \qquad v(r) < v(b).$$

Procédure :

1. On calcule le quotient complexe $\frac{a}{b} = x + iy \in \mathbb{C}$.
2. On arrondit séparément les parties réelles et imaginaires pour obtenir un élément de $\mathbb{Z}[i]$: $q = \lfloor x \rceil + i \lfloor y \rceil$ $\in \mathbb{Z}[i]$
3. On calcule le reste $r = a - b \cdot q$.
4. Par construction [a], $v(r) \leq \frac{1}{2} v(b) < v(b)$.

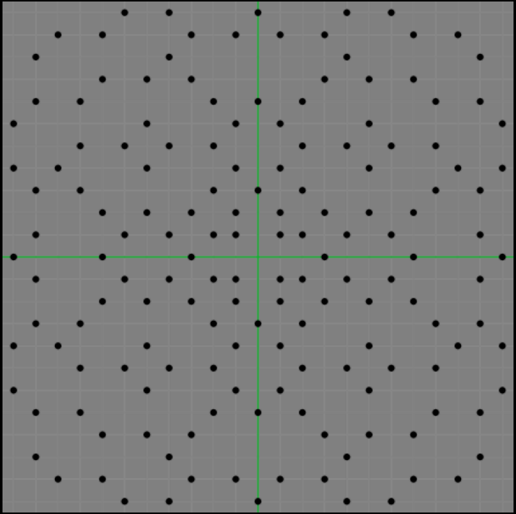
Remarque : Cette méthode revient à ***projeter*** a/b sur le point de la grille de Gauss le plus proche.



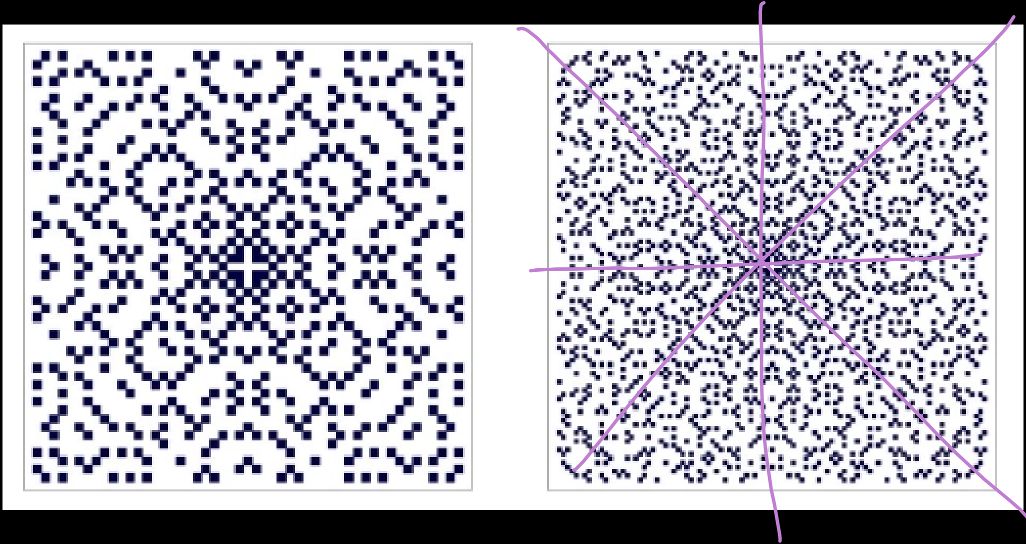
a. Si vous êtes motivés, faites les calculs ou demandez-moi de l'aide.

$v(u+iv) = u^2+v^2 \in \mathbb{Z}$ où $u, v \in \mathbb{Z}$

Les ~~premiers~~ irréductibles de Gauss



Les premiers de Gauss



That's All Folks !

n personnes → partager un secret $b \in \mathbb{Z}$

$n=10$ → le secret est accessible ssi il y a d / 4 / 7 personnes présentes

la personne $i = 1 \dots n$ reçoit un secret x_i

je vais prendre un corps à $> b$ élts, ex : $\mathbb{Z}_p$ où $p > b$

$\mathbb{Z}_p[X]$

P de degré 6 de $\mathbb{Z}_p[X]$

$$P = a_6 X^6 + a_5 X^5 + \dots + a_1 X + b$$

personne $i \Rightarrow P(i)$

$$P(X) = 1 X^6 + 3X^5 + \dots \quad b$$

$\rightarrow P(1)$

$\rightarrow P(2)$

$P(3)$

$\vdots$

$P(10)$

$i \to P(i) \in \mathbb{Z}_p$

inversible du Vandermonde

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0 \\ \vdots & & & & & & \\ 6^6 & 6^5 & 6^4 & 6^3 & 6^2 & 6^1 & 6^0 \end{pmatrix} \begin{pmatrix} a_6 \\ a_5 \\ a_4 \\ a_3 \\ a_2 \\ a_1 \\ b \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_7 \end{pmatrix}$$

$$\left.\begin{array}{l} P(1) = x_1 \\ \vdots \\ P(6) = x_6 \end{array}\right\} \begin{array}{l} a_6 1^6 + \dots + a_1 1 + b = x_1 \\ \vdots \\ a_6 6^6 + \dots + a_1 6 + b = x_6 \end{array}$$