142 PGCD, PPCM, algorithme de calcul. Applications.

Dans cette leçon, A désigne un anneau intègre, commutatif, unitaire. Soit $a \in A$. On écrit (a) l'idéal de A engendré par a.

I) Anneaux factoriels, anneaux principaux:

I.1) Divisibilité:

Déf 1 Soient $a, b \in A$. On dit que a divise b et on note $a|b$ si $\exists c \in A$ tq $b = ac$.

Déf 2 Soit $a \in A$. On dit que a est irréductible si $a \notin A^\times$ et $a = bc \Rightarrow b \in A^\times$ ou $c \in A^\times$. On dit que a est premier si $a \in A^\times$ et $a = bc \Rightarrow a|b$ ou $a|c$.

Rem 3 Dans un anneau intègre, a premier $\Rightarrow$ a irréductible. La réciproque n'est pas vraie.

Déf 4 Soient $a, b \in A$. d est un PGCD de a et b, et on note $d = a \wedge b$, si $d|a$, $d|b$ et si $\exists d'$ tq $d'|a$, $d'|b$, alors $d'|d$. m est un PPCM de a et b et on note $m = a \vee b$ si $a|m$, $b|m$ et si $\exists m'$ tq $a|m'$ et $b|m'$, alors $m|m'$.

Déf 5 Soient $a, b \in A$. a et b sont dits premiers entre eux si $a \wedge b \in A^\times$.

Prop 6 $a \wedge b = d \Leftrightarrow a = da'$ et $b = db'$ avec a' et b' premiers entre eux.

DEV 1: Probabilité que deux entiers soient premiers entre eux.

Rem 7 Un PGCD ou un PPCM n'est pas unique, il l'est à inversible près.

Lemme 8 Soient $a, b \in A$. Si a et b ont un PGCD, ils ont un PPCM. La réciproque est fausse.

Prop 9 Si $d = a \wedge b$ existe alors $a \vee b = \dfrac{uab}{a \wedge b}$ avec $u \in A^\times$.

I.2) Anneau factoriel:

Déf 10 Un anneau A est dit factoriel si $\forall a \in A \setminus A^\times$, $\exists (p_1, \dots, p_r) \in A^r$ irréductible et $u \in A^\times$ tels que $a = u \times p_1 \times \dots \times p_r$. Cette décomposition est unique à l'ordre des facteurs et multiplication par un inversible près.

Prop 11 Dans un anneau factoriel, a premier $\Leftrightarrow$ a irréductible.

Exemple 12 $\mathbb{Z}$ ou $\mathbb{K}[X]$ ($\mathbb{K}$ un corps) sont factoriels.

Prop 13 Dans un anneau factoriel A, deux éléments a et b ont toujours un PGCD et un PPCM.
Soient $a = u \prod_{i=1}^{r} p_i^{\alpha_i}$ et $b = v \prod_{i=1}^{r} p_i^{\beta_i}$.
Alors :
- $a \wedge b = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$
- $a \vee b = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$

Rem 14 On peut ainsi définir le PGCD ou PPCM de n éléments $a_n = u_n \prod_{i=1}^{r} p_i^{\alpha_{ni}}$
- $a_1 \wedge \dots \wedge a_n = \prod_{i=1}^{r} p_i^{\min(\alpha_{1i}, \dots, \alpha_{ni})}$
- $a_1 \vee \dots \vee a_n = \prod_{i=1}^{r} p_i^{\max(\alpha_{1i}, \dots, \alpha_{ni})}$

Exemple 15 On peut construire des ensembles finis d'éléments tous premiers entre eux mais 2 à 2 non premiers entre eux.
Exemple $\{6, 10, 15\}$.

Déf 16 Soit A factoriel. Soit $P \in A[X]$. Le contenu de P est le PGCD de ses coefficients, noté $c(P)$.

Prop 17 $P, Q \in A[X]$. $c(PQ) = c(P)c(Q)$.

Déf 18 Un polynôme P est dit primitif si $c(P) \in A^\times$.

Théorème (de Gauss) 19 Si A est factoriel, alors $A[X]$ l'est aussi et ses irréductibles sont :
- les irréductibles de A.
- les polynômes primitifs de $A[X]$ et irréductibles dans $\mathbb{K}[X]$ avec $\mathbb{K}$ le corps des fraction de A.

I.3) Anneaux principaux:

Déf 20 Un anneau A est dit principal si tous les idéaux I de A peuvent s'écrire $I = (a)$ avec $a \in A$.

Prop 21 A principal $\Rightarrow$ A factoriel.

Prop 22: Soient $a, b \in A$. $a | b \Leftrightarrow (b) \subset (a)$.

Prop 23: Soit $d \in A$ tq $(d) = (a)+(b)$. Alors $a \wedge b = d$.

- Soit $m \in A$ tq $(m) = (a) \cap (b)$. Alors $a \vee b = m$.

Rem 24: On peut généraliser ce résultat à n éléments.

Théorème (relation de Bézout) 25: $d = a_1 \wedge \dots \wedge a_n \Leftrightarrow \exists (u_1, \dots, u_n) \in A^n$ tq $d = a_1 u_1 + \dots + a_n u_n$.

Rem 26: Bézout n'est pas vrai partout. Par exemple, sur $\mathbb{K}[X,Y]$, X et Y sont premiers entre eux mais il n'existe aucun P et Q tels que $P(X,Y)X + Q(X,Y)Y = 1$.

Application : Lemme des noyaux 27: Soit E un $\mathbb{K}$-ev de dim. n. Soit $f \in L(E)$ et $P = P_1 \dots P_r$ avec $P_i \in \mathbb{K}[X]$ 2 à 2 premiers entre eux. Alors $Ker(P(f)) = \bigoplus_{i=1}^{r} Ker(P_i(f))$

Corollaire (lemme de Gauss) 28: Soient a, b, c tels que $a | bc$ et a, b premiers entre eux. Alors $a | c$.

Voyons maintenant quelques méthodes pour calculer efficacement des PGCD.

II) Anneaux euclidiens et algorithmes de calcul :

II.1) Anneaux euclidiens :

Déf 29: Un anneau A est dit euclidien s'il existe un stathme φ, c'est à dire une application $\varphi : A \to \mathbb{N}$ telle que $\forall (a,b) \in A^2, b \neq 0$, $\exists (q, r) \in A^2$ tq $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Prop 30: A euclidien $\Rightarrow$ A principal.

Prop 31: Soit r le reste de la division euclidienne de a par b. Alors $a \wedge b = b \wedge r$.

II.2) Algorithmes :

Algorithme d'Euclide (version récursive) 32: Soient $a, b \in A$ (euclidien). L'algorithme suivant permet de calculer $a \wedge b$: PGCD(a,b) :

- Si $b = 0$ rendre a.
- Sinon, rendre PGCD(b, r) avec r reste de la division euclidienne de a par b.

Cet algorithme construit la suite $(r_n)_n$ des restes : $r_0 = a$, $r_1 = b$ et pour $n > 1$, r_n est le reste de la div. eucl. de r_{n-2} par r_{n-1}. Il s'agit d'une suite strictement décroissante de entiers, elle est donc finie et s'arrête au premier n tel que $r_n = 0$.

Rem 33: Chaque appel recursif entraîne une division euclidienne, de complexité $O(n^2)$ (avec n = nbr de bits dans les nombres d'entrées). Il y a $O(n)$ appels récursifs donc cet algorithme est en $O(n^3)$

Corollaire 34: $a \wedge b$ est le dernier résidu non nul du processus.

Application 35: La réduction à un dénominateur commun de deux polynômes.

Exemple 36: $a = X^2 - 3X + 2$ et $b = X^2 - 1$ dans $\mathbb{Q}[X]$:

$a = 1 \times b - 3X + 3$

$b = \frac{1}{3} X(-3X + 3) + 0$

Donc un PGCD de a et b est $-3X + 3$.

Algorithme d'Euclide étendu 37: Soient $a, b \in A$ (euclidien). L'algorithme suivant calcule le PGCD d de a et b mais aussi les coefficients u et v de la relation de Bézout $au + bv = d$.

- Initialisation : $r_0 = a$, $r_1 = b$, $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$.
- tant que $r_1 \neq 0$:
  - $q := r_0 \div r_1$
  - $rs := r_0$, $us := u_0$, $vs := v_0$ (var. temp.)
  - $r_0 := r_1$, $u_0 := u_1$, $v_0 := v_1$,
  - $r_1 := rs - q r_1$, $u_1 := us - q u_1$, $v_1 = vs - q v_1$

rendre (r_0, u_0, v_0)

Rem 38: Les égalités $r_0 = a u_0 + b v_0$ et $r_1 = a u_1 + b v_1$ sont des invariants de boucle.

Rem 39: La complexité d'Euclide étendu est la même que celle d'Euclide, à une constante multiplicative près.

Algorithme binaire (40) : L'algorithme suivant permet de calculer le PGCD de deux entiers a et b de façon récursive :
Si $b=0$ rendre a
Si a et b sont pairs, rendre $2\times PGCD(a/2, b/2)$
Si a impair et b pair, rendre $PGCD(a, b/2)$
Si a pair et b impair, rendre $PGCD(a/2, b)$
Si a et b impairs, rendre $PGCD((a-b)/2, b)$

Exemple (41) : $PGCD(30,24) = 2\times PGCD(15,12)$
$= 2\times PGCD(15,6) = 2\times PGCD(15,3)$
$= 2\times PGCD(6,3) = 2\times PGCD(3,3)$
$= 2\times PGCD(0,3) = 2\times 3 = 6$

III) Applications :

III.1) Équations diophantiennes :

Théorème (42) : Soient $a,b,c \in \mathbb{Z}$.
L'équation $ax+by=c$ admet des solutions dans $\mathbb{Z}^2 \Leftrightarrow d=a\wedge b$ divise c.
Dans ce cas l'ensemble des solutions est l'ensemble de couples $(x,y)=(x_0+bk/d, y_0-ak/d)$ où $k\in\mathbb{Z}$ et (x_0,y_0) est une solution particulière de l'équation (donnée par l'algorithme d'Euclide étendu).

Exemple (43) : $6x+9y=5$ n'a pas de solution dans $\mathbb{Z}^2$.
$3x+2y=7$ a pour solution les $(7+2k, 7-3k)$, $k\in\mathbb{Z}$.

III.2) Restes chinois et systèmes de congruences :

$\boxed{\text{DEV 2}}$: Théorème des restes chinois

Théorème des restes chinois (dans $\mathbb{Z}/n\mathbb{Z}$) (44) :
Soient n, m deux entiers. Alors n et m sont premiers entre eux ssi $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$

Exemple (45) : $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$
mais $\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Application (46) Résolution d'un système de congruences de la forme :
$$(S) : \begin{cases} x \equiv a\,[m] \\ x \equiv b\,[n] \end{cases}$$

Théorème des restes chinois (dans un anneau principal) (47) : Soient $a_1,\dots,a_k \in A$ (principal) 2 à 2 premiers entre eux et $a = a_1\cdots a_k$. Alors le morphisme d'anneau :
$$f : A/aA \longrightarrow A/a_1A\times\dots\times A/a_kA$$
$$x \bmod aA \longmapsto (x \bmod a_1A, \dots, x \bmod a_kA)$$
est un isomorphisme.

Application (48) : L'interpolation de Lagrange est un cas particulier du théorème appliqué à la résolution d'un système de congruence dans l'anneau euclidien $\mathbb{K}[X]=A$
$\forall i\in\{0,\dots,n\}$, $P \equiv P_i \bmod A_i$
avec les A_i de la forme $X-x_i$ et les P_i constants.

III.3) Calcul d'inverses :

Prop (49) : Soit $n\in\mathbb{N}^*$. Alors $\bar{a}_n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $a\wedge n=1$.
Dans ce cas, l'inverse de $\bar{a}_n$ est $\bar{u}_n$ où u est le coefficient de a dans la relation de Bézout $au+nv=1$.

Exemple (50) : 4 est inversible dans $\mathbb{Z}/9\mathbb{Z}$ et $4^{-1}=-2$ (ou -7).

Prop (51) : Soit $P\in\mathbb{K}[X]$ avec $\mathbb{K}$ un corps. Soit $\bar{Q}\in\mathbb{K}[X]/(P)$. Alors $\bar{Q}$ est inversible ssi Q est premier avec P dans $\mathbb{K}[X]$.
En particulier, si P est irréductible, alors $\mathbb{K}[X]/(P)$ est un corps.