Kit de survie pour les leçons

103 - L'anneau $\mathbb{Z}/n\mathbb{Z}$. Applications

106 - PGCD dans $\mathbb{Z}$ et $\mathbb{K}[X]$, Bezout, applications.

I. PGCD dans $\mathbb{Z}$ et $\mathbb{K}[X]$. Bezout. Euclide

Rappel : $\mathbb{Z}$ et $\mathbb{K}[X]$ et des anneaux **euclidiens**

Tout idéal de $\mathbb{Z}$ ou de $\mathbb{K}[X]$ est **principal**.

Conséquence : . Si $a, b \in \mathbb{Z}^*$, il existe un unique $d \in \mathbb{N}^*$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

. Si $P, Q \in \mathbb{K}[X]^*$, il existe un unique polynôme unitaire D tel que $P\mathbb{K}[X] + Q\mathbb{K}[X] = D\mathbb{K}[X]$.

$d = \text{pgcd}(a,b)$; $D = \text{pgcd}(P,Q)$.

Théorème (Bezout)

- $\text{pgcd}(a,b) = 1$ $\Leftrightarrow \exists u, v \in \mathbb{Z}$, $au + bv = 1$
- $\text{pgcd}(P,Q) = 1 \Leftrightarrow$ $\exists U, V \in \mathbb{K}[X]$, $PU + QV = 1$

- Si $d = \text{pgcd}(a,b)$,
  $\exists u, v \in \mathbb{Z}$, $au + bv = d$
- Si $D = \text{pgcd}(P,Q)$,
  $\exists U, V \in \mathbb{K}[X]$, $PU + QV = D$.

Corollaire "pgcd = pgcd":

$\forall \delta \in \mathbb{Z}$, $\delta | a$ et $\delta | b$
$\Leftrightarrow \delta | \text{pgcd}(a,b)$

$\forall \Delta \in \mathbb{K}[X]$, $\Delta | P$ et $\Delta | Q$
$\Leftrightarrow \Delta | \text{pgcd}(P,Q)$.

Algorithme d'Euclide : permet de déterminer le pgcd (et) une relation de Bezout.

Repose sur le fait que :

$\text{pgcd}(a,b) = \text{pgcd}(b,r)$ où r est le reste de la division euclidienne de a par b.

Exercice d'application : *

Pour tout a, m, n

$$\text{pgcd}(a^n - 1, a^m - 1) = a^{\text{pgcd}(n,m)} - 1$$

Corollaire (de Bezout) : Gauss.

Si $a \mid bc$ et si $\text{pgcd}(a,b) = 1$, alors $a \mid c$.

"Relations de Bezout"

Soit $a, b \in \mathbb{Z}$, $d = \text{pgcd}(a,b)$

Si $au_0 + bv_0 = d$ est une relation de Bezout, alors toute relation de Bezout est de la forme $au + bv = d$

avec $u = u_0 + \frac{b}{d}n$; $v = v_0 - \frac{a}{d}n$

où $n \in \mathbb{Z}$.

* Indication : Montrer que le reste de la division euclidienne de $a^n - 1$ par $a^m - 1$ est $a^r - 1$ où r est le reste de la division euclidienne de n par m. Puis Euclide.

II Applications dans $\mathbb{K}[X]$.

1) (Voir les notes sur la leçon 165)

Calcul de l'inverse de $x \in \mathbb{Q}(\alpha) \setminus \{0\}$ où α est un entier algébrique.

2) Théorème des noyaux.

Soit E un $\mathbb{K}$-ev, $u \in \mathcal{L}(E)$

Soit $P_1, \dots, P_r \in \mathbb{K}[X]$ deux à deux premiers entre eux. Alors :

$$\operatorname{Ker}(P_1 \dots P_r)(u) = \bigoplus_{i=1}^{r} \operatorname{Ker}(P_i(u)).$$

3) Décomposition en éléments simples.

Si $\operatorname{pgcd}(P,Q) = 1$, $R = PU + QV$

$$\frac{R}{PQ} = \frac{PU+QV}{PQ} = \frac{U}{Q} + \frac{V}{P}.$$

4) Résultant de deux polynômes

Soit $P \in \mathbb{K}[X]$, $\deg P = n$

$Q \in \mathbb{K}[X]$, $\deg Q = m$.

Soit $A : K_{m-1}[X] \times K_{n-1}[X] \to K_{m+n-1}[X]$

$(U, V) \longmapsto PU + QV$

Soit S la matrice de A dans les bases $((X^{m-1}, 0), \dots, (1,0), (0, X^{n-1}), \dots, (0,1))$ et $(X^{m+n-1}, \dots, 1)$.

(a) Montrer que A est un isomorphisme si et seulement si $\text{pgcd}(P,Q) = 1$.

On note $\text{Res}(P,Q) = \det S$ (résultant de P et Q).

(b) Calculer $\text{Res}(P,P')$ avec $P = aX^2 + bX + c$ puis $P = X^3 + pX + q$.

Commenter.

III Applications dans $\mathbb{Z}$

1) Résolution d'équations diophantiennes

$ax + by = c$ $\quad \underbrace{a,b,c}_{\text{données}}, \underbrace{x,y}_{\text{inconnues}} \in \mathbb{Z}$

2) "Problèmes de calendrier".

Un astronome observe le jour J_0 un corps céleste A qui apparaît tous les 105 jours. Au jour J_0+6, il observe le corps B qui apparaît tous les 81 jours. Déterminer le jour J_1 de la prochaine apparition simultanée des deux corps A et B.

D'autres applications trouvent leur place dans l'étude de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

IV L'anneau $\mathbb{Z}/n\mathbb{Z}$

1) • $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif, de cardinal n.

• Inversible de $\mathbb{Z}/n\mathbb{Z}$:

$\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow pgcd(k,n) = 1$

Un calcul de l'inverse de $\overline{k}$ est effectué à l'aide de Bezout.

$Card((\mathbb{Z}/n\mathbb{Z})^*) = \varphi(n)$ (Indicatrice d'Euler)

- Structure de $\mathbb{Z}/n\mathbb{Z}$ et théorème chinois.

si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, (déc. en facteurs premiers)

alors $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$

et $(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^*$.

- Euler : si $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $x^{\varphi(n)} \equiv 1 \ [n]$

2) $\mathbb{Z}/p\mathbb{Z}$ avec $p \in \mathcal{P}$

Thm $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si $p \in \mathcal{P}$.

Petit thm de Fermat :

$\forall x \in \mathbb{Z}/p\mathbb{Z}$, $x^p = x$ (dans $\mathbb{Z}/p\mathbb{Z}$)

$\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$, $x^{p-1} = 1$ (dans $\mathbb{Z}/p\mathbb{Z}$).

Thm (plus délicat, mais développement possible pour plein de leçons).

$(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique (de cardinal $p-1$).

Exercice Montrer que

$$\operatorname{card}(GL_n(\mathbb{Z}/p\mathbb{Z})) = (p^n-1)\times(p^n-p)\times\cdots\times(p^n-p^{n-1})$$

$$\operatorname{card}(SL_n(\mathbb{Z}/p\mathbb{Z})) = \frac{1}{p-1}\times \operatorname{card}(GL_n(\mathbb{Z}/p\mathbb{Z}))$$

Application :

Soit G un sous-groupe fini de $GL_n(\mathbb{Z})$

Soit $p \in \mathcal{P}$, $p \geq 3$

1) Montrer que $G \longrightarrow GL_n(\mathbb{Z}/p\mathbb{Z})$

$M \longmapsto \overline{M}^p$

↑ réduction modulo p coeff par coeff.

est injective.

2) En déduire que

$$\operatorname{card}(G) \leq (3^n-1)\times\cdots\times(3^n-3^{n-1}).$$

3) Algorithme de cryptage RSA.

Résultat préliminaire :

Si $n = pq$ $p, q \in \mathcal{P}$,

montrer que : $\forall x \in \mathbb{Z}, \forall k \in \mathbb{N}, \forall M \in \mathbb{Z}$,

$$M^{1+k\varphi(n)} \equiv M \ [n].$$

Principe du cryptage RSA.

. Bob choisit $p, q \in \mathbb{P}$, puis un nombre c tel que $\text{pgcd}(c, \varphi(n)) = 1$.

Bob rend public c et $n = pq$

. Alice veut envoyer $x \in \mathbb{Z}/n\mathbb{Z}$ à Bob.

Elle lui envoie $y = x^c$.

. Bob détermine d et u tels que

$$cd + \varphi(n)u = 1 \quad \text{(Bezout)}$$

Puis calcule $y^d = ?$

Exemple $p = 5$, $q = 11$, $c = 3$; $x = 4$.

4) L'anneau $\mathbb{Z}[i]$, les carrés modulo p et les nombres premiers congrus à 1 modulo 4.

Voir les notes spécifiques.

5) Une application du thm chinois

Exercice 17 pirates + 1 cuisinier + 1 trésor de pièces d'or.

Si le trésor est partagé équitablement entre les 17 pirates, il reste 3 pièces d'or pour le cuisinier.

Les pirates se disputent → 6 tués. Un nouveau partage équitable entre les pirates restants conduirait à un reste de 4 pièces pour le cuisinier.

Le bateau coule : il reste 6 pirates et le cuisinier, qui gagneraient alors 5 pièces.

Le cuisinier décide d'empoisonner tout le monde et récupère tout le trésor. Combien récupère-t-il de pièces d'or ?