Développement : Théorèmes Chinois et applications.

RM

2022-2023

Référence :

1. Algèbre Perrin
2. algèbre Rombaldi

Énoncé :

Soit $\mathbb{A}$ un anneau unitaire principal. Soit $(a_j)_{1\leq j\leq r}$ des éléments non nuls inversibles deux à deux premiers entre eux avec $a=\prod_{i=1}^{r} a_j$. Alors l'application $\varphi : x\in\mathbb{A}\mapsto (\pi_j(x))_{1\leq j\leq r}\in\prod_{i=1}^{r}\frac{\mathbb{A}}{(a_j)}$ est un morphisme d'anneaux surjectif de noyau $Ker(\varphi)=(a)$. et φ induit un isomorphisme d'anneaux

$$\overline{\varphi} : \pi(x)\in\frac{\mathbb{A}}{(a)}\mapsto (\pi_j(x))_{1\leq j\leq r}\in\prod_{i=1}^{r}\frac{\mathbb{A}}{(a_j)}$$

d'inverse

$$\overline{\varphi}^{-1} : (\pi_j(x_j))_{1\leq j\leq r}\in\prod_{i=1}^{r}\frac{\mathbb{A}}{(a_j)}\mapsto\overline{\sum_{i=1}^{r} x_i u_i b_i}\in\frac{\mathbb{A}}{(a)}$$

où $(u_j)_{1\leq j\leq r}$ est une suite d'éléments de $\mathbb{A}$ telle que $\sum_{i=1}^{r} u_j b_j = 1$.

Lemme 1 : On appelle $(b_j)_{1\leq j\leq r}$ la suite d'éléments de $\mathbb{A}$ définie par $b_j=\frac{a}{a_j}=\prod_{\substack{i=1\\ i\neq j}}^{r} a_i$. Si les a_j sont deux à deux premiers entre eux pour $j\in[\![1\,;r]\!]$, les b_j sont alors premiers entre eux dans leur ensemble.

Démonstration : Si les b_j ne sont pas premier entre eux dans leur ensemble, il existe alors un élément premier p de $\mathbb{A}$ qui divise tous les b_j (l'anneau $\mathbb{A}$ étant principal est factoriel). Comme p divise $b_1=\prod_{i=2}^{r} a_i$, il divise un a_i pour $i\in[\![2\,;r]\!]$, mais divisant b_i, il divise un a_k pour $1\leq k\neq i\leq r$, ce qui contredit le fait que a_i et a_k sont premiers entre eux. □

Résolution :

Démonstration : Il est clair que l'application $\varphi : x\in\mathbb{A}\mapsto (\pi_j(x))_{1\leq j\leq r}\in\prod_{j=1}^{r}\frac{\mathbb{A}}{(a_j)}$ est un morphisme d'anneaux. Son noyau est formé des multiples de tous les a_j, donc de leur ppcm $a=\prod_{j=1}^{r} a_j$ puisque les a_j sont deux à deux premiers eux. Comme les $b_i=\frac{a}{a_i}$ sont premiers entre eux dans leur ensemble (lemme précédent), le théorème de Bézout nous dit qu'il existe une suite $(u_i)_{1\leq i\leq r}$ d'éléments de $\mathbb{A}$ telle que $\sum_{i=1}^{r} u_i b_i = 1$. Pour $1\leq j\leq r$, on a $\pi_j(b_i)=\pi_j(0)=0$ pour $i\neq j$ puisque b_i est multiple de a_j, ce qui nous donne $\pi_j(1)=1=\pi_j\left(\sum_{i=1}^{r} u_i b_i\right)=\pi_j(u_j)\pi_j(b_j)$. Donc $\pi_j(b_j)$ est inversible dans $\frac{\mathbb{A}}{(a_j)}$ d'inverse $\pi_j(u_j)$.
Pour $(\pi_j(x_j))_{1\leq j\leq r}$ donné dans $\prod_{j=1}^{r}\frac{\mathbb{A}}{(a_j)}$, en posant $x=\sum_{i=1}^{r} x_i u_i b_i$, on a $\pi_j(x)=\pi_j(x_j)\pi_j(u_j)\pi_j(b_j)=\pi_j(x_j)$ pour tout $j\in[\![1\,;r]\!]$, soit $\varphi(x)=(\pi_j(x_j))_{1\leq j\leq r}$. Le morphisme φ est donc surjectif et il se

factorise en un isomorphisme (grâce au premier théorème d'isomorphisme) :

$$\begin{array}{rccc} \overline{\varphi}: & \frac{\mathbb{A}}{(a)} = \frac{\mathbb{A}}{ker(\varphi)} & \to & \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)} \\ & \pi(x) & \mapsto & (\pi_j(x))_{1\leq j\leq r} \end{array}$$

Avec la surjectivité, on a prouvé que l'inverse de $\overline{\varphi}$ est défini par :

$$\begin{array}{rccc} \overline{\varphi}^{-1}: & \prod_{j=1}^{r} \frac{\mathbb{A}}{(a_j)} & \to & \frac{\mathbb{A}}{(a)} \\ & (\pi_j(x_j))_{1\leq j\leq r} & \mapsto & \sum_{i=1}^{r} x_i u_i b_i \end{array}$$

□

Application (Calcul de $\varphi(n)$) 2 : Si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $2 \leq p_1 < ... < p_r$ premiers et les α_i entiers naturels non nuls, on a alors :

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Lemme 3 : Pour tout nombre premier p et tout entier naturel non nul α, on a $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Démonstration : Si p est premier, alors un entier k compris entre 1 et p^α n'est pas premier avec p^α si, et seulement si, il est divisible par p, ce qui équivaut à $k = mp$ avec $m \in [\![1\,; p^{\alpha-1}]\!]$, il y a donc $p^{\alpha-1}$ possibilités. On en déduit que :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$$

□

Démonstration (Théorème) : Le théorème chinois nous fournit l'isomorphisme suivant :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \prod_{j=1}^{r} \frac{\mathbb{Z}}{p_j^{\alpha_j}\mathbb{Z}}$$

On a alors un isomorphisme de groupe entre les inversibles qui nous donne

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \cong \left(\prod_{j=1}^{r} \frac{\mathbb{Z}}{p_j^{\alpha_j}\mathbb{Z}}\right)^\times = \prod_{j=1}^{r} \left(\frac{\mathbb{Z}}{p_j^{\alpha_j}\mathbb{Z}}\right)^\times$$

En prenant les cardinaux, on en déduit $\varphi(n) = \prod_{i=1}^{r} \varphi(p_j^{\alpha_j})$.
On a d'après le lemme la première égalité. On trouve la deuxième en factorisant par pj :

$$\prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = \prod_{i=1}^{r} pi^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

□

Application (Résolution d'un système de congruence) 4 : On considère le système suivant :

$$\begin{cases} k \equiv 2[4] \\ k \equiv 3[5] \\ k \equiv 1[9] \end{cases}$$

Alors $k = 118 + 180q$ ou $q \in \mathbb{Z}$ est solution du système.

Démonstration : Comme $n_1 = 4$,$n_2 = 5$ et $n_3 = 9$ sont deux à deux premiers entre eux,

ce système a des solutions données en déterminant des coefficients dans une relation de Bézout $u_1m_1 + u_2m_2 + u_3m_3 = 1$, où $m_1 = n_2n_3 = 45$,$m_2 = n_1n_3 = 36$,$m_3 = n_1n_2 = 20$. Pour ce faire, on utilise l'associativité du *pgcd* en écrivant que :

$$\begin{cases} m_2 \wedge m_3 = 4 = (-1).36 + 2.20 \\ 1 = m_1 \wedge (m_2 \wedge m_3) = 1.45 + (-11).4 \\ 1 = 1.45 + 11.36 + (-22).20 \end{cases}$$

Ce qui donne une solution particulière $k_0 = 2.45 + 33.36 - 22.20 = 838$ et comme $838 \equiv 118[180]$, on trouve bien la solution. □