Théorème des restes chinois et application :

I Le développement

Le but de ce développement est de démontrer le théorème des restes chinois (grâce à un lemme préliminaire) dans le but de résoudre des systèmes d'équations diophantiennes dans $\mathbb{Z}/n\mathbb{Z}$ par exemple.

Dans tout ce développement, on considère $(A, +, \times)$ un anneau commutatif principal.
On commence tout d'abord par démontrer un lemme qui sera utile pour la preuve du théorème :

Lemme 1 : [Rombaldi, p.249]
Soient $a_1, ..., a_r$ des éléments de A deux à deux premiers entre eux.
Si l'on pose, pour tout $i \in [\![1; r]\!]$, $b_i = \prod_{\substack{j=1 \\ j\neq i}}^{r} a_j$, alors les b_i sont premiers entre eux dans leurs ensemble.

Preuve :
Soient $a_1, ..., a_r$ des éléments de A deux à deux premiers entre eux.
Pour tout $i \in [\![1; r]\!]$, on pose $b_i = \prod_{\substack{j=1 \\ j\neq i}}^{r} a_j$.
On raisonne par l'absurde en supposant que les b_i ne soient pas premiers entre eux dans leur ensemble.
Il existe alors un élément premier p de A qui divise tous les b_j (car l'anneau A est principal et donc factoriel). Ainsi, comme p divise $b_1 = \prod_{i=2}^{r} a_i$, il divise un a_i (car deux à deux premiers entre eux). Mais il divise aussi b_i (pour $i \neq 1$) et donc l'un des a_k pour $k \neq i$, ce qui contredit le fait que a_i et a_k sont premiers entre eux.

Ainsi, les b_i sont premiers entre eux dans leur ensemble.

■

On peut désormais passer à la preuve du théorème :

Théorème 2 : Théorème des restes chinois [Rombaldi, p.249] :
Soient $a_1, ..., a_r$ des éléments de A deux à deux premiers entre eux.
L'application :

$$\varphi : \left| \begin{array}{ccc} A & \longrightarrow & \prod_{i=1}^{r} A/(a_i) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array} \right.$$

est un morphisme d'anneaux surjectif de noyau $\left(\prod_{i=1}^{r} a_i\right)$.

On a donc en particulier :

$$A\Big/\left(\prod_{i=1}^{r} a_i\right) \cong \prod_{i=1}^{r} A/(a_i)$$

Preuve :
Soient $a_1, ..., a_r$ des éléments de A deux à deux premiers entre eux.
On considère l'application :

$$\varphi : \left| \begin{array}{ccc} A & \longrightarrow & \prod_{i=1}^{r} A/(a_i) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array} \right.$$

Montrons que φ est un morphisme d'anneaux surjectif de noyau $\left(\prod_{i=1}^{r} a_i\right)$:

$*$ φ est bien un morphisme d'anneaux (car il s'agit de projections coordonnées par coordonnées).

$*$ Soit $x \in A$.

$$x \in \mathrm{Ker}(\varphi) \iff \forall i \in [\![1; r]\!],\ \pi_i(x) = 0 \iff \forall i \in [\![1; r]\!],\ a_i \text{ divise } x$$
$$\iff \mathrm{PPCM}(a_1, ..., a_r) \text{ divise } x \iff \prod_{j=1}^{r} a_j \text{ divise } x \iff x \in \left(\prod_{j=1}^{r} a_j\right)$$

On a donc $\mathrm{Ker}(\varphi) = \left(\prod_{j=1}^{r} a_j\right)$.

$*$ Pour tout $i \in [\![1;r]\!]$, on pose $b_i = \prod_{\substack{j=1 \\ j\neq i}}^{r} a_j$.

Les b_j sont premiers entre eux dans leur ensemble, donc par le théorème de Bézout, il existe $u_1, ..., u_r$ des éléments de A tels que $\sum_{i=1}^{r} b_i u_i = 1_A$.

Pour tout $j \in [\![1;r]\!]$, on a $\pi_j(b_i) = 0_{A/(a_j)}$ pour $i \neq j$ (car b_i est multiple de a_j), ce qui donne :

$$\pi_j(1_A) = \pi_j\left(\sum_{i=1}^{r} u_i b_i\right) = \pi_j(u_j)\pi_j(b_j) = 1_{A/(a_j)}$$

Donc $\pi_j(b_j)$ est inversible dans $A/(a_j)$, d'inverse $\pi_j(u_j)$.

Pour $(\pi_j(x_j))_{j\in[\![1;r]\!]}$ donné dans $\prod_{i=1}^{r} A/(a_i)$, en posant $x = \sum_{i=1}^{r} x_i u_i b_i$, on a pour tout $j \in [\![1;r]\!]$:

$$\pi_j(x) = \pi_j(x_j)\pi_j(u_j)\pi_j(b_j) = \pi_j(x_j)$$

Et donc $\varphi(x) = (\pi_j(x_j))_{j\in[\![1;r]\!]}$ et donc φ est surjectif.

Finalement, φ est donc un morphisme d'anneaux surjectif et noyau $\left(\prod_{i=1}^{r} a_i\right)$ et par le théorème d'isomorphisme :

$$A\Big/\left(\prod_{i=1}^{r} a_i\right) \cong \prod_{i=1}^{r} A/(a_i)$$

■

On donne désormais notre application :

Exemple 3 : [Rombaldi, p.291]

On considère le système d'équations diophantiennes suivant :

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

Le but est de trouver les antécédents de $(\overline{2}, \overline{3}, \overline{1})$ par l'application :

$$\varphi : \left|\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \\ x & \longmapsto & (\pi_4(x), \pi_5(x), \pi_9(x)) \end{array}\right.$$

Or, le théorème des restes chinois nous donne les antécédents : il nous suffit donc de déterminer u_4, u_5 et u_9 grâce à une relation de Bézout à 3 coefficients.

On a :

$$45 - 36 = 9(5-4) = 9 \text{ et } \begin{cases} 20 = 2 \times 9 + 2 \\ 9 = 4 \times 2 + 1 \end{cases}$$

Ainsi :

$$\begin{aligned} 1 &= 9 - 4 \times 2 = 9 - 4 \times (20 - 2 \times 9) \\ &= 9 - 4 \times 20 + 8 \times 9 = 9 \times 9 - 4 \times 20 = 9 \times 45 - 9 \times 36 - 4 \times 20 \end{aligned}$$

On a alors $u_4 = 9$, $u_5 = -9$ et $u_9 = -4$ et donc les solutions de (S) sont exactement les $118 + 180n$, avec $n \in \mathbb{Z}$.

II Remarques sur le développement

II.1 Pour aller plus loin...

On sait que si l'on a deux anneaux unitaires A et B et φ un isomorphisme d'anneaux de A sur B, alors φ induit un isomorphisme de groupes de $A^\times$ sur $B^\times$.

En particulier, en décomposant $n = \prod_{j=1}^{r} p_j^{a}{}_j$ (décomposition en facteurs premiers), le théorème des restes chinois nous donne alors :

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/p_j^{a_j}\mathbb{Z}$$

d'où :

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \left(\prod_{i=1}^{r} \mathbb{Z}/p_j^{a_j}\mathbb{Z}\right)^\times = \prod_{i=1}^{r} \left(\mathbb{Z}/p_j^{a_j}\mathbb{Z}\right)^\times$$

En particulier, en prenant les cardinaux, on obtient que $\varphi(n) = \prod_{i=1}^{r} \varphi\left(p_j^{a_j}\right)$.

II.2 Recasages

Recasages : 120 - 121 - 122 - 142.

III Bibliographie

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et géométrie*.