Développement : Théorème des restes chinois et applications

Algèbre & Géométrie

Références : [ROM] Rombaldi J., *Mathématiques pour l'agrégation - Algèbre et géométrie*, 2ème édition, deobeck supérieur, 2021, p249.

Pour les leçons :
- 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 122 : Anneaux principaux. Exemples et applications.
- 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Soit A un anneau principal. $\mathbb{P}$ désigne l'ensemble des nombres premiers (dans $\mathbb{Z}$).
Le but de ce développement est de démontrer le théorème suivant :

Théorème 1. ***des restes chinois.***

Soient $r \in \mathbb{N}^*$ et $a_1, \dots, a_r \in A$ premiers entre eux deux à deux, non nuls et non inversibles. Soit $\varphi : A \to A/(a_1) \times \cdots \times A/(a_r)$ l'application dont les applications coordonnées sont la réduction modulo a_j, pour $j \in [\![1; r]\!]$.
Alors, φ est un morphisme d'anneaux surjectif de noyau $\mathrm{Ker}(\varphi) = \left(\prod_{j=1}^{r} a_j\right)$, et induit un isomorphisme d'anneaux $\bar{\varphi} : A/\mathrm{Ker}(\varphi) \longrightarrow A/(a_1) \times \cdots \times A/(a_r)$.

Lemme 2.

On garde les notations du théorème. Pour $j \in [\![1; r]\!]$, on pose $b_j = \dfrac{a}{a_j} = \prod_{\substack{i=1 \\ i \neq j}}^{r} a_i$. Alors, les b_j sont premiers entre eux dans leur ensemble.

Preuve : Raisonnons par l'absurde en supposant que les b_j ne sont pas premiers entre eux dans leur ensemble. Comme A est principal (donc factoriel), il existe $p \in A$ premier divisant tous les b_j.
Comme $p | b_1 = \prod_{i=2}^{r} a_i$, et comme les a_i sont premiers entre eux, d'après le lemme d'Euclide, il existe $i \in [\![2; r]\!]$ tel que $p | a_i$.
Mais $p | b_i$, donc p divise $\prod_{\substack{j=1 \\ j \neq i}}^{r} a_j$. Le lemme d'Euclide donne encore l'existence de $k \in [\![1; r]\!] \backslash \{i\}$ tel que $p | a_k$.
On a donc $p | a_k$ et $p | a_i$, ce qui est absurde puisque $a_k \wedge a_i = 1$. Les b_j sont donc premiers entre eux dans leur ensemble. □

Preuve du théorème : Déjà, φ est un morphisme d'anneaux. Ensuite, en notant $\Pi_j : x \longmapsto x \bmod(a_j)$:

$$\begin{aligned}
\mathrm{Ker}(\varphi) &= \{x \in A \mid \forall j \in [\![1; r]\!] \quad \Pi_j(x) = 0\} \\
&= \{x \in A \mid \forall j \in [\![1; r]\!] \quad a_j | x\} \\
&= \left\{x \in A \mid \prod_{j=1}^{r} a_j \mid x\right\} \\
&= \left(\prod_{j=1}^{r} a_j\right),
\end{aligned}$$

puisque les a_j sont premiers entre eux deux à deux.
Ensuite, les $b_i = \dfrac{a}{a_i}$ sont premiers entre eux dans leur ensemble d'après le théorème précédent. D'après le théorème de Bézout :

$$\exists u_1, \dots, u_r \in A \quad \sum_{i=1}^{r} u_i b_i = 1.$$

Soit $j \in [\![1; r]\!]$. Pour tout $i \in [\![1; r]\!] \backslash \{j\}$, comme $a_j | b_i$, on a $\Pi_j(b_i) = 0$. Donc :

$$\begin{aligned}
\Pi_j(1) &= \Pi_j\left(\sum_{i=1}^{r} u_i b_i\right) \\
&= \sum_{i=1}^{r} \Pi_j(u_i)\Pi_j(b_i) \\
1 &= \Pi_j(u_j)\Pi_j(b_j),
\end{aligned}$$

et donc $\Pi_j(b_j) \in (A/(a_j))^\times$, d'inverse $\Pi_j(u_i)$.

Maintenant, si $(\Pi_j(x_j))_{1\leqslant j\leqslant r} \in \prod_{j=1}^r A/(a_j)$, posons $x = \sum_{i=1}^r x_i u_i b_i$.

Soit $j \in [\![1;r]\!]$. On a, de la même manière que précédemment, $\Pi_j(x) = \Pi_j(x_j) \underbrace{\Pi_j(u_j)\Pi_j(b_j)}_{=1 \text{ par ce qui précède}} = \Pi_j(x_j)$.

Ainsi, $\varphi(x) = (\Pi_j(x_j))_{1\leqslant j\leqslant r}$, et φ est un morphisme d'anneaux surjectif.
D'après le premier théorème d'isomorphisme, φ induit une bijection $\bar{\varphi} : A/\mathrm{Ker}(\varphi) \longrightarrow A/(a_1) \times \cdots \times A/(a_r)$. □

Lemme 3.

Pour tout $p \in \mathbb{P}$ et $\alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Preuve : Si $p \in \mathbb{P}$, alors pour tout $k \in [\![1;p^\alpha]\!]$, on a :

$$k \wedge p^\alpha \neq 1 \iff p|k \iff \exists m \in [\![1;p^{\alpha-1}]\!] \quad k = mp.$$

Il y a donc $p^{\alpha-1}$ possibilités pour k. Ainsi, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$. □

Application 4.

Si $n \geqslant 2$ s'écrit $n = \prod_{i=1}^r p_i^{\alpha_i}$, où les $p_i \in \mathbb{P}$ tels que $2 \leqslant p_1 < \cdots < p_r$, et les $\alpha_i \in \mathbb{N}^*$, alors :

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

Preuve : D'après le théorème des restes chinois, $\mathbb{Z}/n\mathbb{Z} \cong \prod_{j=1}^r \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$.

Donc, en tant que groupe, $(\mathbb{Z}/n\mathbb{Z})^\times \cong \left(\prod_{j=1}^r \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}\right)^\times = \prod_{j=1}^r (\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^\times$.

Par conséquent, $\varphi(n) = \prod_{j=1}^r \varphi(p_j^{\alpha_j}) = \prod_{j=1}^r p_i^{\alpha_i - 1}(p_i - 1)$.

En factorisant par $p_i^{\alpha_i}$ à l'intérieur du produit, sachant que $n = \prod_{i=1}^r p_i^{\alpha_i}$, on obtient le résultat. □

Application 5.

Soit (E) le système $\begin{cases} k \equiv 2[4] \\ k \equiv 3[5] \\ k \equiv 1[9] \end{cases}$. Les solutions entières de (E) sont de la forme $k = 118 + 180q$, où $q \in \mathbb{Z}$.

Preuve : Soient $n_1 = 4$, $n_2 = 5$, $n_3 = 9$. n_1, n_2, n_3 sont premiers entre eux deux à deux.
D'après le théorème des restes chinois, les solutions sont données en déterminant les coefficients de Bézout pour $4 \times 5 = 20$, $4 \times 9 = 36$ et $5 \times 9 = 45$.
Déjà, $20 \wedge 36 = 4 = 36 \times (-1) + 20 \times 2$.
Ensuite, $1 = 20 \wedge 36 \wedge 45 = 45 \times 1 + 4 \times (-11)$. Donc, en remplaçant 4 par son expression précédente :

$$1 = 45 \times 1 + 36 \times 11 + 20 \times (-22).$$

On pose $k_0 = 45 \times 1 \times 2 + 36 \times 11 \times 3 + 20 \times (-22) \times 1 = 838 \equiv 118[180]$. D'après le théorème des restes chinois, l'ensemble des solutions est $118 + 180\mathbb{Z}$. □