Théorème chinois

Rombaldi, p.249, 291

Théorème : Soit A un anneau principal, $a_1, \dots, a_r \in A \setminus \{A^\times \cup \{0\}\}$ 2-à-2 premiers entre eux.
Alors $\overline{\varphi} : \begin{array}{rcl} A/(a_1 \cdots a_r) & \longrightarrow & A/(a_1) \times \cdots \times A/(a_r) \\ \pi(x) & \longmapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$ est un isomorphisme d'anneaux,
d'inverse $\overline{\varphi}^{-1} : \begin{array}{rcl} A/(a_1) \times \cdots \times A/(a_r) & \longrightarrow & A/(a_1 \cdots a_r) \\ (\pi_1(x_1), \dots, \pi_r(x_r)) & \longmapsto & \pi\left(\sum_{i=1}^r x_i u_i b_i\right) \end{array}$ où $\sum_{i=1}^r u_i b_i = 1$ avec $b_i = \prod_{j \neq i} a_j$

L'application $\varphi : \begin{array}{rcl} A & \longrightarrow & A/(a_1) \times \cdots \times A/(a_r) \\ x & \longmapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$ est un morphisme d'anneaux car les π_i en sont

Noyau : On a : $\mathrm{Ker}\, \varphi = \{x \in A ; \forall 1 \leq i \leq r, \pi_i(x) = 0\} = \{x \in A ; \forall 1 \leq i \leq r, x \in (a_i)\} = \bigcap_{i=1}^r (a_i) \overset{\text{par définition du ppcm}}{=} (\mathrm{ppcm}(a_1, \dots, a_r))$
Or, les a_i sont 2-à-2 premiers entre eux donc $\mathrm{ppcm}(a_1, \dots, a_r) = a_1 \cdots a_r$.

Surjectivité : Montrons que les b_i sont premiers entre eux dans leur ensemble.
Si par l'absurde ils ne le sont pas, il existe $p \in A$ irréductible tel que $p \mid b_i, \forall 1 \leq i \leq r$. → A principal $\Rightarrow A$ factoriel
Or, $p \mid b_1 = a_2 \cdots a_r$ donc par Euclide, $\exists 2 \leq i \leq r$ tel que $p \mid a_i$. Mais $p \mid b_i = \prod_{j \neq i} a_j$ donc $\exists 1 \leq j \neq i \leq r$ tel que $p \mid a_j$. Donc $p \mid a_i$ et $p \mid a_j$. Or, a_i et a_j sont premiers entre eux. $\Rightarrow \Leftarrow$
Il existe alors une relation de Bézout : soit $u_1, \dots, u_r \in A$ tels que $\sum_{i=1}^r u_i b_i = 1$.
D'où, $\forall 1 \leq j \leq r$, $\pi_j(u_j)\pi_j(b_j) = \pi_j(1)$. $\forall i \neq j, \pi_j(u_i b_i) = \pi_j(u_i)\underbrace{\pi_j(b_i)}_{=0}$
Soit $(\pi_1(x_1), \dots, \pi_r(x_r)) \in A/(a_1) \times \cdots \times A/(a_r)$. Posons $x = \sum_{i=1}^r x_i u_i b_i \in A$. D'après la remarque ci-dessus, on a :
$\forall 1 \leq j \leq r, \quad \pi_j(x) = \pi_j(x_j) \underbrace{\pi_j(u_j)\pi_j(b_j)}_{=1} = \pi_j(x_j)$
D'où $\varphi(x) = (\pi_1(x_1), \dots, \pi_r(x_r))$ et φ est surjectif.

Factorisation : Par le 1er théorème d'isomorphisme, $\overline{\varphi} : \begin{array}{rcl} A/(a_1 \cdots a_r) & \longrightarrow & A/(a_1) \times \cdots \times A/(a_r) \\ \pi(x) & \longmapsto & (\pi_1(x), \dots, \pi_r(x)) \end{array}$ est un isomorphisme d'anneaux. On a montré au passage l'expression de $\overline{\varphi}^{-1}$.

Application : Les solutions du système $\begin{cases} k \equiv 2 \pmod 4 \\ k \equiv 3 \pmod 5 \\ k \equiv 1 \pmod 9 \end{cases}$ sont de la forme $118 + 180n$ où $n \in \mathbb{Z}$.

On a $n_1 = 4$, $n_2 = 5$ et $n_3 = 9$ qui sont 2-à-2 premiers entre eux.
On cherche alors l'antécédent de $(\pi_4(2), \pi_5(3), \pi_9(1))$ dans $\mathbb{Z}/4\times5\times9\mathbb{Z} = \mathbb{Z}/180\mathbb{Z}$ par l'isomorphisme
$\varphi : \begin{array}{rcl} \mathbb{Z}/180\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \\ \pi_{180}(k) & \longmapsto & (\pi_4(k), \pi_5(k), \pi_9(k)) \end{array}$. Cet antécédent $\overline{k}_0$ est donné par $k_0 = 2u_1 \overbrace{\tfrac{180}{4}}^{=45} + 3u_2 \overbrace{\tfrac{180}{5}}^{=36} + 1u_3 \overbrace{\tfrac{180}{9}}^{=20}$
On cherche alors une relation de Bézout entre 20, 36 et 45 :
On a : $36 \wedge 20 = 4 = 2\times20 - 36$ et $1 = 20 \wedge 36 \wedge 45 = 4 \wedge 45 = 45 - 11\times4 = 45 - 11(2\times20 - 36)$
$45 = 4\times11 + 1 \Rightarrow 45 - 4\times11 = 1$
$36 = 1\times20 + 16$, $20 = 1\times16 + 4$, $16 = 4\times4 + 0$
$\Rightarrow 4 = 20 - 1\times16 = 20 - (36 - 20) = 2\times20 - 36$
$= 1\times45 + 11\times36 - 22\times20$
D'où $k_0 = 2\times1\times45 + 3\times11\times36 - 1\times22\times20 = 838$
$\Rightarrow \overline{k}_0 = \pi_{180}(838) = 118$
$\Rightarrow$ Donc l'ensemble des solutions est $k_0 + 180\mathbb{Z} = 118 + 180\mathbb{Z}$.