Théorème chinois

Théorème : Soit A un anneau principal et $a_1, ..., a_r \in A \setminus (A^\times \cup \{0\})$. On pose $a = a_1...a_r$. Si les a_i sont premiers entre eux l'application

$$\psi : \begin{array}{ccc} A/(a) & \to & A/(a_1) \times ... \times A/(a_r) \\ x \mod a & \mapsto & (x \mod a_1, ..., x \mod a_r) \end{array}$$

est un isomorphisme d'anneaux. De plus il existe $u_1, ..., u_r \in A$ tels que $\sum_{i=1}^{r} u_i \frac{a}{a_i} = 1$ et l'inverse de ψ soit donné par

$$\psi^{-1} : \begin{array}{ccc} A/(a_1) \times ... \times A/(a_r) & \to & A/(a) \\ (x_1 \mod a_1, ..., x_r \mod a_r) & \mapsto & \sum_{i=1}^{r} x_i u_i \frac{a}{a_i} \end{array}.$$

On notera $b_i = \frac{a}{a_i}$ dans la suite.

Application 1 : Si $n = p_1^{\alpha_1}...p_r^{\alpha_r}$, en notant φ l'indicatrice d'Euler, on a

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)...p_r^{\alpha_r - 1}(p_r - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Application 2 : Les nombres de la forme $k = 118 + 180q$, où $q \in \mathbb{Z}$, sont les seules solutions du système suivant :

$$\begin{cases} k = 2 \mod 4 \\ k = 3 \mod 5 \\ k = 1 \mod 9 \end{cases}.$$

Preuve du théorème : Posons l'application

$$\varphi : \begin{array}{ccc} A & \to & A/(a_1) \times ... \times A/(a_r) \\ x & \mapsto & (x \mod a_1, ..., x \mod a_r) \end{array}.$$

On commence par vérifier que φ est bien un morphisme d'anneau. C'est bien le cas car les applications $x \mapsto x \mod a_i$ le sont, ce n'est alors pas compliqué de voir que le "produit" de ces applications est comme voulu.

On voit maintenant que $\ker(\varphi) = \{x \in A : a_1|x, ..., a_r|x\} = \{x : \text{ppcm}(a_1, ..., a_r)|x\}$. Si on suppose les a_i premiers entre eux on sait que $\text{ppcm}(a_1, ..., a_r) = a$ et donc $\ker(\psi) = aA$. Le théorème de factorisation nous dit alors que l'on peut quotient φ de sorte à avoir ψ bien définit et injectif.

Montrons que ψ est surjectif. On se donne $(x_1 \mod a_1, ..., x_r \mod a_r) \in A/(a_1) \times ... \times A/(a_r)$. Comme les a_i sont premiers entre eux, les b_i le sont aussi (si p divise tous les b_i, il divise en particulier b_1 donc $p|a_k$ pour $k > 1$. Mais $p|b_k$ donc divise a_l pour $l \neq k$, absurde). Comme nous sommes dans un anneau principal le théorème de Bézout nous dit qu'il existe $u_1, ...u_r \in A$ tels que

$$\sum_{i=1}^{r} u_i b_i = 1.$$

Soit alors $x = \sum_{i=1}^{r} x_i u_i b_i$. On a alors $\psi(x) = (x_1 u_1 b_1 \mod a_1, ..., x_r u_r b_r \mod a_r)$. De plus on remarque que $1 \mod a_i = u_i b_i \mod a_i$ avec la relation de Bézout donc $\psi(x) = (x_1 \mod a_1, ..., x_r \mod a_r)$. On vient de montrer la surjectivité en donnant l'inverse. $\square$

Preuve de l'application 1 : On sait que $\varphi(p^{\alpha}) = p^{\alpha-1}(p-1)$ et comme $\mathbb{Z}$ est principal on va pouvoir utiliser le théorème chinois, à savoir

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}.$$

Cela nous donne aussi un isomorphisme de groupe sur les inversibles et donc pas égalité des cardinaux il vient $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^{\times} = \prod_{i=1}^{r} \#(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^{\times} = \prod_{i=1}^{r} \varphi(p^{\alpha_i})$. On a alors le résultat après une petite simplification :

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

Preuve de l'application 2 : On cherche en fait la classe d'équivalence de $\mathbb{Z}/180\mathbb{Z}$ dont l'image par l'isomorphisme ψ est $(2 \mod 4, 3 \mod 5, 1 \mod 9)$. Pour ça, il faut trouver les coefficients de Bézout u_1, u_2, u_3 tels que

$$45u_1 + 36u_2 + 20u_3 = 1.$$

Comme le pgcd est associatif on cherche des coefficients au fur et à mesure : On voit que $36 \wedge 20 = 4 = 2 \times 20 + (-1) \times 36$ et $45 \wedge (36 \wedge 20) = 1 = 1 \times 45 + (11) \times 4 = 1 \times 45 + 11 \times 36 + (-22) \times 20$.

La classe d'équivalence recherchée est donc $(2 \times 45 \times 1) + (3 \times 36 \times 11) + (1 \times 20 \times (-22)) \mod 180 = 838 \mod 180 = 118 \mod 180. \square$

Remarques importantes :

- Aussi triviales semblent-elles, il faut faire attention à toutes les petites propriétés utilisées sur les pgcd, ppcm ect.
- Faites des tests au niveau du temps, les 2 applications sont potentiellement trop longues.
- J'ai supposé connu l'indicatrice d'Euler sur les puissances de nombres premiers, il faut savoir le faire.