Développement : Théorème des restes Chinois

Référence : Carnet de voyage en Algébrie
Leçon : 120, 122 et 142.

Théorème :
Soit $n, m \in \mathbb{Z}$. On a : n et m sont premiers entre eux si et seulement si les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.

Démonstration. $\star$ Sens direct. Supposons que n et m sont premiers entre eux. Considérons l'application entre anneau $\tilde{\varphi} : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ définie par $\tilde{\varphi}(x) = (\bar{x}_m, \bar{x}_n)$

L'application $\tilde{\varphi}$ est un morphisme.

L'entier x est dans $\ker(\tilde{\varphi})$ si et seulement si $(\bar{x}_m, \bar{x}_n) = (\bar{0}_m, \bar{0}_n)$. Cela est vraie si et seulement si m divise x et n divise x. Par la propriété fondamentale du ppcm, il revient donc à dire que le ppcm de m et n divise x. Comme m et n sont premiers entre eux cela équivaut à la condition mn divise x.
Nous avons donc montré l'égalité $\ker(\tilde{\varphi}) = mn\mathbb{Z}$. On passe au quotient (par le théorème d'isomorphisme). On obtient un morphisme φ injective et comme $|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|$ on a φ est bijective.

$\star$ Sens réciproque. Supposons les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes. Notons encore g cette application.

Soit μ le ppcm de m et n. On voit que $\mu(\bar{a}_m, \bar{b}_n) = (\mu\bar{a}_m, \mu\bar{b}_n) = (\bar{0}_m, \bar{0}_n)$ pour tout $(\bar{a}_m, \bar{b}_n)$ de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En appliquant l'isomorphisme inverse g^{-1}, on obtient que $\mu\bar{x}_{nm} = \bar{0}_{nm}$ pour tout x dans $\mathbb{Z}$; en particulier, pour $x = 1$. On trouve donc $\mu = 0$ modulo mn. Or, μ divise mn par suite $\mu = mn$. Comme le pgcd de m et n est égal à mn/μ, cela implique que m et n sont premiers entre eux. □

Proposition :
Soit a, b dans $\mathbb{Z}$; on considère le système de congruence

$$(S) : \begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases}$$

où m et n sont premiers entre eux. Alors, l'ensemble de solution est $\{(avn+bum)+kmn \mid k \in \mathbb{Z}\}$ où (v, u) sont les coefficients de Bézout de m et n

Démonstration. Posons Si x est solution de (S) alors $\varphi(\bar{x}_{mn}) = (\bar{a}_m, \bar{b}_n)$. D'après l'identité de Bézout, avec m et n premiers entre eux, il existe u et v dans $\mathbb{Z}$ tels que :

$$um + vn = 1$$

On a donc

$$um \equiv 0 \ [m], \quad um \equiv 1 \ [n]$$

et ainsi $\tilde{\varphi}(um) = (\bar{0}_m, \bar{1}_n)$. De même,

$$vn \equiv 1 \ [m], \quad vn \equiv 0 \ [n]$$

et ainsi $\tilde{\varphi}(vn) = (\bar{1}_m, \bar{0}_n)$

Comme $(\bar{a}_m, \bar{b}_n) = a(\bar{1}_m, \bar{0}_n) + b(\bar{0}_m, \bar{1}_n) = a\tilde{\varphi}(vn) + b\tilde{\varphi}(mu)$ et comme $\tilde{\varphi}$ est un morphisme, l'élément $x := a(vn)+b(um)$ vérifie $\tilde{\varphi}(x) = (\bar{a}_m, \bar{b}_n)$. Par passage au quotient $\varphi(\bar{x}_{mn}) = (\bar{a}_m, \bar{b}_n)$ De plus comme φ est bijectif, cette solution est unique. La solution de (S) est donc :

$$\{(avn + bum) + kmn \mid k \in \mathbb{Z}\}.$$

□

Exemple :
Résoudre dans $\mathbb{Z}$ le système

$$(S) : \begin{cases} x \equiv 6 \ [12] \\ x \equiv 13 \ [19] \end{cases}$$

Démonstration. Les entiers 12 et 19 étant premiers entre eux, leurs ppcm est donc $12\times19 = 228$. Déterminons des coefficients de Bézout ; on trouive par exemple $8 \times 12 - 5 \times 19 = 1$. On a donc

$$-6 \times 5 \times 19 + 13 \times 8 \times 12 = 678$$

L'ensemble de solution de notre système de congruence est donc

$$\{678 + 228k \mid k \in \mathbb{Z}\} = \{222 + 228k \mid k \in \mathbb{Z}\}.$$

□