Niveau : 1 **Jaune**

Le théorème des restes chinois

1 Présentation du problème

Il s'agit d'étudier ce qu'il se passe lorsqu'on travaille avec deux modules. Autrement dit si on a une relation entre deux entiers qui est vraie modulo m et modulo n, que peut on en conclure.

Théorème 1.1 *Si m et n sont premiers entre eux alors la condition :*

$$\begin{cases} a \equiv b & (m) \\ a \equiv b & (n) \end{cases}$$

est équivalente à :

$$a \equiv b \quad (mn).$$

Preuve. Si $a \equiv b \quad (mn)$ les deux relations $a \equiv b \quad (m)$ et $a \equiv b \quad (n)$ ont bien lieu.
Réciproquement si ces deux relations ont lieu alors il existe k_1 et k_2 tels que :

$$a - b = k_1 m = k_2 n.$$

On voit alors que m divise $k_2 n$ et comme il est premier avec n il divise k_2. Si bien que :

$$a - b = k_3 mn.$$

2 Théorème des restes chinois

Soient m et n premiers entre eux. On cherche toutes les solutions entières de :

$$\begin{cases} x \equiv a & (m) \\ x \equiv b & (n) \end{cases}$$

On considère u et v tels que $um + vn = 1$.

Théorème 2.1 *(Théorème des restes chinois) On obtient une solution en prenant :*

$$x = bum + avn.$$

Toutes les solutions sont alors de la forme :

$$x + kmn.$$

Preuve. Par un calcul direct on vérifie que $x = bum + avn$ est bien une solution. On vérifie alors que pour tout entier k, $x + kmn$ est aussi une solution.
Si maintenant x et y sont deux solutions par différence on obtient :

$$\begin{cases} x \equiv y & (m) \\ x \equiv y & (n) \end{cases},$$

ce qui nous permet de conclure :

$$y = x + kmn$$

grâce au théorème **??**.1.1.
Remarque: Il y a donc une solution unique y vérifiant $0 \leq y < mn$; ce qui peut s'exprimer encore en disant qu'il y a une unique solution dans $\mathbb{Z}/mn\mathbb{Z}$.

Théorème 2.2 *L'anneau $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Preuve. En appliquant le théorème précédent on montre que l'application T de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ définie par :

$$T(x \mod mn) = ((x \mod m), (x \mod n))$$

est un isomorphisme d'anneaux.
Remarquons que la classe de x modulo mn est inversible modulo mn si et seulement si les classes de x modulo m et modulo n sont inversibles respectivement modulo m et modulo n.