Théorème Chinois:

On se propose de montre l'isomorphisme d'anneaux suivant, pour (n_i) des nombres premiers entre eux et n le produit de ces nombres:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$$

On considère l'application suivante:

$$\begin{aligned} \phi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \\ x[n] &\longmapsto (x[n_1], \ldots, x[n_k]) \end{aligned}$$

Alors, on montre facilement par les propriétés des congurences que ϕ est **un morphisme d'anneaux**. Il reste à montrer qu'il est bijectif, pour cela on remarque tout d'abord que les deux ensembles (finis) ont le même cardinal, il reste alors à montrer l'injectivité.

On se donne alors x tel que $(x[n_1], \ldots, x[n_k]) = 0$, alors x est divisible par tout les n_i et ils sont premiers entre eux, on en déduis donc que x est divisible par leur produit.

Petit théorème de Fermat:

On se propose de montrer la propriété suivante pour p premier et pour tout entier a:

$$a^p \equiv a[p]$$

Par récurrence sur a, on a directement l'initialisation et si on suppose le résultat vrai pour $a \geq 0$, alors on a que:

$$(a+1)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1$$

Or, on peut alors montrer, en utilisant **la formule du capitaine** et le **lemme de Gauss** que si p est premier, on a:

$$\forall k \in [\![1\ ;\ p-1]\!]\ ;\ p \left| \binom{p}{k} \right.$$

Donc finalement les termes de la somme disparaissent modulo p et on obtient:

$$(a+1)^p \equiv a^p + 1 \underset{HR}{\equiv} a + 1$$

En particulier, si a est inversible modulo p (ie si a est premier avec p), alors on a:

$$a^{p-1} \equiv 1[p]$$