Arithmetique | CM: 8

Par Lorenzo

08 novembre 2024

Théorème 0.1. *Soient $n_1, n_2, ..., n_k \in \mathbb{N}^*$, tels que $\forall i, n_i \geq 2$, avec les n_i deux à deux premiers entre eux. Alors pour tous $a_1, ..., a_k \in \mathbb{Z}$, il existe $x \in \mathbb{Z}$, unique modulo $n := \Pi n_i$, tel que*

$$\forall i \in [|1, k|], x \equiv a_i mod n_i$$

Plus formellement, on a une application bijective,

$$\{\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \times ... \times (\mathbb{Z}/n_k\mathbb{Z})\{x mod n \mapsto (x mod n_1, ..., x mod n_k)$$

Démonstration 0.1.

Montrons deja que
$PGCD(\Pi_{i=1}^{k-1} n_i, n_k) = 1$
Soit p un facteur premier de $\Pi_{i=1}^{k-1} n_i$ Alors p divise l'un des n_i.
Comme n_i et n_k sont premier entre eux p ne divise pas nk.
Donc $\Pi_{i=1}^{k-1} n_i$ et n_k n'ont pas de facteur premier en commun : leurs PGCD est 1.
De même pour $i \in [|1; k|]$ $PGCD(\Pi_{i \neq j} n_j, n_i) = 1$.
Ainsi on pose une relation de Bezout

$$(\Pi_{i \neq j} n_j) u_i + n_i v_i = 1$$

Soit $x_i := (\Pi_{j \neq i} n_j) u_i$
Alors $x_i \equiv \{0 mod n_j si j \neq i\{1 mod n_i$
On pose $x = \Sigma_{i=1}^{k} a_i x_i$ alors $x \equiv a_i mod n_i$
Si $y = x + qn$ alors $y = x + q\Pi_{j=1}^{k} n_j = x + q(\Pi_{j=1}^{k} n_j) n_i \equiv x mod n_i \equiv x_i mod n_i$
En particulier l'application ϕ est bien définie
D'après la première partie, ϕ est surjective.
Il nous reste à démontrer l'injectivité qui est equivalente à l'unicité modulo n.
Regardons les cardinaux $Card(\mathbb{Z}/n\mathbb{Z}) = n$
$Card(\mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}) = n_1 \times ... \times n_k = n$
Ainsi ϕ est injective

□

Remarques 0.1. *ϕ est un "isomorphisme" d'anneau*

Pour $k = z$

$$\{x \equiv a_1 mod n_1 \{x = a_1 + k_1 n_1 \{x \equiv a_2 mod n_2 \iff \{x = a_2 + k_2 n_2$$

Alors $a_1 + k_1 n_1 = a_2 + k_2 n_2 \iff k_1 n_1 - k_2 n_2 = a_2 - a_1$
c'est une équation diophotienne qu'on sait résoudre
Ensuite, il suffit de poser $x = a_1 + k_1 n_1$

1 Polynômes et Fractions rationnelles

Définition 1.1. *Un **polynôme à coefficient dans** $\mathbb{k}$: une suite $A = (a_n)_{n\in\mathbb{N}}$ telle que $\exists N \in \mathbb{N}, \forall n > N, a_n = 0$.*

On écrira souvent $A = a_0 + a_1 X + a_2 X^2 + ... + a_N X^N = \Sigma_{i=0}^{N} a_i X^i = \Sigma_{i\in\mathbb{N}} a_i X^i = \Sigma a_i X^i$

$\mathbb{k}[X]$ = {polynômes à coefficients dans $\mathbb{k}$}

***polynôme nul** : tous les coefficients sont nuls.*

***polynôme constant** : $\forall i > 0, a_i = 0$ ($A = cX^0 = c$ où $c \in \mathbb{k}$)*

***monôme** : polynôme de la forme*

Symbole de Kronecker $\delta_{i,j} = 1$ si i = j sinon 0