Fiche de révisions chapitre 5 : Restes chinois & Euler.

I. Théorème des restes chinois

1) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

- $x \equiv a_i \mod m_i$ avec $i = 1, \dots, n$ et $PGCD(m_i, m_j) = 1$ $i \neq j$

Posons $M = \prod_{i=1}^{n} m_i$ Alors :

1) $\Pi : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z} : [X + M\mathbb{Z}] \to ([x + m_1\mathbb{Z}], [x + m_2\mathbb{Z}], \dots, [x + m_n\mathbb{Z}])$ est un isomorphisme d'anneau

ex : $[X + 55\mathbb{Z}] \to ([X + M\mathbb{Z}], [X + 5\mathbb{Z}])$

2) Le système a pour ensemble de solution $X_0 + M\mathbb{Z}$.

$$X_0 = \sum_{i=1}^{n} a_i \cdot M_i \cdot N_i \text{ avec } M_i = \frac{M}{m_i} \text{ et } N_i = M_i^{-1} \mod m_i$$

II. Euler.

Indicatrice d'Euler : $\Psi : \mathbb{N} \to \mathbb{N}$ définie par $\Psi(n) = \#\{a \in \mathbb{N} \mid a \leq a < n \text{ et } PGCD(a, n) = 1\}$

$$\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right| = \Psi(n)$$

$\Psi(m \times n) = \Psi(m) \times \Psi(n)$

$\Psi(1) = 1$
$\Psi(p^\alpha) = p^\alpha - p^{\alpha-1}$ } si p premier
$\Psi(p) = p - 1$.

$[a + n\mathbb{Z}]^{\Psi(n)} = [1 + n\mathbb{Z}]$ si $PGCD(a, n) = 1$

$[a + p\mathbb{Z}]^{p-1} = [1 + n\mathbb{Z}]$ si p premier

Rappel :

20	2
10	2
5	5

- trouver les éléments inversibles : ex : 20 $\phi(20) = \phi(2^2 \times 5^1) = (2^2 - 2)(5^1 - 5^0)$
  ↳ on cherche les nombres non divisibles par les facteurs premiers de n. $\phi(20) = (4-2)(5-1) = 2 \times 4 = 8$
  $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$

156	2
78	2
39	3
13	13
1	

- calcul de Euler : $\phi(p) = p - 1$; $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$
  $\phi(156) = \phi(2^2 \times 3^1 \times 13^1) = (2^2 - 2^1)(3^1 - 3^0)(13^1 - 13^0)$
  $\phi(156) = (4-2)(3-1)(13-1) = 2 \times 2 \times 12 = 4 \times 12 = 48$

- $a^{p-1} \equiv 1 \ [p]$ } Fermat
  $a^p \equiv a \ [p]$ }
  $a^{\phi(n)} \equiv 1 \ [n]$ } Euler