Rappel : Soit $n \geq 2$. Le groupe $(\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ est formé des classes $\overline{x}$ inversibles, i.e que x est inversible modulo n, i.e $\text{pgcd}(x, n) = 1$

La loi du groupe est la multiplication des classes

$$\overline{x} \cdot \overline{y} = \overline{xy}$$

Exemple :

$$(\mathbb{Z}/10\mathbb{Z})^* = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

$$\overline{3} \cdot \overline{7} = \overline{21} = \overline{1}$$

Def : $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$

On appelle φ l'indicatrice d'Euler

Remarque : On sait que si G est un groupe d'ordre n alors tout élément $g \in G$ est d'ordre fini et son ordre n

Donc on a

$$\boxed{g^n = e, \forall g \in G}$$

On applique ceci au groupe $G = (\mathbb{Z}/n\mathbb{Z})^*$ pour obtenir le

Théorème 2.20 : Soit x premier avec n. Alors

$$x^{\varphi(n)} \equiv 1 \bmod n$$

Déf : Dans $G = (\mathbb{Z}/n\mathbb{Z})^*$, on a $\overline{x}^{\varphi(n)} = \overline{1}$

Cette égalité dans $(\mathbb{Z}/n\mathbb{Z})^*$ se traduit par la congruence
$$x^{\varphi(n)} \equiv 1 \bmod n$$

Corollaire : Si x est premier avec n et $e \in \mathbb{Z}$ alors $\boxed{x^e \bmod n}$ ne dépend pas de $e \bmod \varphi(n)$

Prop 2.22

a) Si $\text{pgcd}(n,m) = 1$, alors $\varphi(nm) = \varphi(n)\varphi(m)$
En particulier, si $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ pour des nombres premiers p_i distincts 2 à 2 et des exposants $e_i \geq 1$, alors
$$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \dots \varphi(p_r^{e_r})$$

b) Si p est premier et $e \geq 1$, alors
$$\varphi(p^e) = p^e - p^{e-1}$$

Exemple : Soit $n = 3072$. On a $n = 3072$
$= 3 \times 1024$
$= 3 \times 2^{10}$

Donc
$$\varphi(n) = \varphi(2^{10} \cdot 3) = \varphi(2^{10})\varphi(3)$$
$$= (2^{10} - 2^9)(3^1 - 3^0)$$
$$= 2^9 \cdot 2 = 2^{10} = 1024$$

Démonstration de la prop : b) Il s'agit de compter les classes $\bar{x}$ dans $\mathbb{Z}/p^e\mathbb{Z}$, les entiers $x \in \{0, \dots p^e - 1\}$ qui sont premiers avec p^e

Comme p est premier, on a
$\text{pgcd}(x, p^e) > 1 \iff p$ divise x

Donc les x tq $\text{pgcd}(x, p^e) = 1$ sont les $x \in \{0, \dots, p^e - 1\}$ qui ne sont pas divisibles par p. Or parmi $0, \dots, p^e - 1$, il y a exactement $p^e / p = p^{e-1}$ qui sont divisibles par p

Donc le nombre de $x \in \{0, \dots, p^e - 1\}$ non divisibles par p est

$$p^e - p^{e-1}$$

Soit $\overline{nm}^{nm} x \in \mathbb{Z}/nm\mathbb{Z}$

Comme $\text{pgcd}(n, m) = 1$, on a

$$\text{pgcd}(x, nm) = 1 \overset{(*)}{\Leftrightarrow} \begin{cases} \text{pgcd}(x, n) = 1 \\ \text{pgcd}(x, m) = 1 \end{cases}$$

Soit

$$\Pi : \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$\overline{x}^{nm} \longmapsto (\overline{x}^{n}, \overline{x}^{m})$$

Comme $\text{pgcd}(n, m) = 1$, l'application Π est bijective grâce au théorème chinois

Par $(*)$, cette bijection induit une bijection

$$(\mathbb{Z}/nm\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

Donc

$$\underbrace{|(\mathbb{Z}/nm\mathbb{Z})^*|}_{\varphi(nm)} = |(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*|$$
$$= \underbrace{|(\mathbb{Z}/n\mathbb{Z})^*|}_{\varphi(n)} \cdot \underbrace{|(\mathbb{Z}/m\mathbb{Z})^*|}_{\varphi(m)}$$

Application : l'algo de chiffrement RSA

C'est un algo inventé en 1978

L'algo permet de chiffrer un message sans disposer de l'information nécessaire pour déchiffrer

(Algo de cryptographie asymétrique)

Il repose sur le fait qu'est facile de multiplier deux grands entiers (plusieurs centaines de chiffres) mais très difficile de factoriser un entier

Alice veut recevoir un message chiffré de Bob qu'elle sache déchiffré mais que personne d'autre (y compris Bob) ne sache déchiffrer.

Elle procède ainsi :

1) Elle choisit deux grands nombres premiers $p \neq q$ ($\geq$ 300 chiffres) et calcule $n = pq$

2) Elle calcule $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q)$
$= (p-1)(q-1)$

3) Elle choisit e, l'exposant de chiffrement, comme un entier $< \varphi(n)$ et premier avec $\varphi(n)$

4) Elle calcule d, l'exposant de déchiffrement comme entiers inverse de d modulo $\varphi(n)$ tq $d < \varphi(n)$
(algo d'Euclide $\rightsquigarrow$ éq de Bézout entre e et $\varphi(n)$:
$d \cdot e + k\varphi(n) = 1$)

La clé publique : d'Alice est le couple (n, e). Elle la publie et, en particulier, la communique à Bob.

La clé privée d'Alice est le couple (n, d). Elle la garde secrète.

Bob code son message sous forme de bloc entiers $M \in \{0, \dots, n\}$ et premiers avec n (Algo d'Euclide permet le vérifier sans connaître pour q)

Bob chiffre M en calculant

$$S = M^e \bmod n$$

Il envoie S à Alice. Alice déchiffre S en calculant

$$S^d \bmod n$$

Elle retrouve bien M car

$$S^d \equiv (M^e)^d \equiv M^{e \cdot d} \equiv M^1 \bmod n$$

$e \cdot d \equiv 1 \bmod \varphi(n)$!

2.4 Homomorphismes, isomorphismes

Def. 2.23 : Soient (G_i) et (H_i^*) deux groupes. Un morphisme (= homomorphisme) de (G_i) vers (H_i^*) est une application

$$f : G \longrightarrow H$$

telle que l'on a

$$f(x \cdot y) = f(x) * f(y), \quad \forall x, y \in G$$

Un morphisme f est un isomorphisme si l'application $f : G \longrightarrow H$ est bijective

Exemple : L'exponentielle

$$f = \exp : \mathbb{R} \longrightarrow \mathbb{R}_{>0}, \; x \longmapsto e^x$$

est un morphisme du groupe $(\mathbb{R}, +)$ vers $(\mathbb{R}_{>0}, \cdot)$ car on a :

$$f(x+y) = e^{x+y} = e^x e^y = f(x) \cdot f(y)$$

f est même un isomorphisme