Applications à l'arithmétique.

Définition. Fonction d'EULER

Soit $n \in \mathbb{N}^*$. Alors on définit

$$\varphi(n) = \left| \{ 0 < k \leq n \mid \mathrm{PGCD}(k,n) = 1 \} \right|$$

Ainsi : $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$

Rappel : $\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \{ \bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{PGCD}(k,n) = 1 \ ; 0 < k \leq n \}$
$n > 1$

On a $\left| \left(\mathbb{Z}/n\mathbb{Z}\right)^* \right| = \varphi(n)$.

Théorème : 1) Soient n_1, n_2 deux entiers premiers entre eux alors $\varphi(n_1 n_2) = \varphi(n_1) \cdot \varphi(n_2)$

2) Soit $n \in \mathbb{N}^*$. Alors

$$\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ premier}}} \left(1 - \frac{1}{p}\right)$$

Preuve : 1) D'après le théorème des restes chinois on a un isomorphisme d'anneaux

$$\Phi : \mathbb{Z}/n_1 n_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

De plus Φ induit une bijection entre les inversibles de $\mathbb{Z}/n_1 n_2\mathbb{Z}$ et $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$

donc on a un isomorphisme de groupes

$$\Phi^* : \left(\mathbb{Z}/n_1 n_2\mathbb{Z}\right)^* \xrightarrow{\sim} \left(\mathbb{Z}/n_1\mathbb{Z}\right)^* \times \left(\mathbb{Z}/n_2\mathbb{Z}\right)^*.$$

d'où $\quad \varphi(n_1 n_2) = \varphi(n_1)\cdot\varphi(n_2)$

2) On peut factoriser $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ en produit de nombres premiers $\alpha_i \in \mathbb{N}^*$, p_i premier, $p_i \neq p_j$ si $i \neq j$.

Alors d'après (1) on a :

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i})$$

car $p_i^{\alpha_i}$ et $p_j^{\alpha_j}$ sont premiers entre eux, si $i \neq j$.

On montre maintenant que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ pour tout nombre premier p et α entier.

$$\varphi(p^\alpha) = \left|\left\{0 < k \leqslant p^\alpha \;\middle|\; \underset{\displaystyle \Updownarrow \atop \displaystyle PGCD(k,p)=1}{PGCD(k,p^\alpha) = 1}\right\}\right|$$

$$= p^\alpha - \left|\left\{0 < k \leqslant p^\alpha \;\middle|\; \underset{\displaystyle \Updownarrow \atop \displaystyle p \mid k \iff k = p\cdot k'}{PGCD(k,p) \neq 1}\right\}\right|$$

or $\quad 0 < p\cdot k' \leqslant p^\alpha$

$$\iff 0 < k' \leqslant p^{\alpha-1} = \frac{p^\alpha}{p}$$

$$= p^\alpha - \left|\left\{0 < k' \leqslant p^{\alpha-1}\right\}\right|$$

$$= p^\alpha - p^{\alpha-1}.$$

Donc, on obtient.

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i} - p_i^{\alpha_i - 1} = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

$$= n \cdot \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) \qquad \square$$

Prop. : Soit G un groupe et $g \in G$ un élément d'ordre. $\mathrm{ord}_G(g) = r$. Alors.

$$\mathrm{ord}_G(g^n) = \frac{r}{\mathrm{PGCD}(r,n)}$$

Preuve : On a

$$(g^n)^{\frac{r}{\mathrm{PGCD}(r,n)}} = g^{\frac{rn}{\mathrm{PGCD}(r,n)}} = (g^r)^{\frac{n}{\mathrm{PGCD}(r,n)}} = e$$

Donc $\frac{r}{\mathrm{PGCD}(r,n)}$ est un multiple de $\mathrm{ord}_G(g^n)$.

Soit $k \in \mathbb{N}$ tel que $(g^n)^k = g^{nk} = e$

Alors d'après ~~le~~ un résultat vu précédemment, nk est un multiple de $\mathrm{ord}_G(g) = r$.

$$\iff r \mid nk$$

$$\iff \frac{r}{\mathrm{PGCD}(r,n)} \mid \frac{n}{\mathrm{PGCD}(r,n)} \cdot k.$$

Donc $\frac{r}{\mathrm{PGCD}(r,n)} \mid k$, d'après le lemme de Gauss.

car $\mathrm{PGCD}\left(\frac{r}{\mathrm{PGCD}(r,n)}, \frac{n}{\mathrm{PGCD}(r,n)}\right) = 1$.

en particuler. $\frac{r}{\mathrm{PGCD}(r,n)} \mid \mathrm{ord}_G(g^n) = k$

ce qui implique $\frac{r}{\mathrm{PGCD}(r,n)} = \mathrm{ord}_G(g^n)$. $\square$

Théorème : Si G est cyclique et fini, alors G admet exactement $\varphi(|G|)$ générateurs.

Preuve : On a $G = \langle g \rangle = \{ g^k \mid 0 \leq k < |G| \}$.

D'après la proposition précédente $r = \mathrm{ord}_G(g) = |G|$.

$$\mathrm{ord}_G(g^k) = \frac{r}{\mathrm{PGCD}(r,k)} = \frac{|G|}{\mathrm{PGCD}(|G|,k)}.$$

Ainsi g^k est un générateur de $G \Leftrightarrow \mathrm{PGCD}(|G|,k) = 1$.

Donc $|\{ 0 \leq k < |G| \ ; \ g^k \text{ générateur} \}|$

$= |\{ 0 \leq k < |G| \ ; \ \mathrm{PGCD}(|G|, k) = 1 \}| = \varphi(|G|)$

$\square$

Théorème (Cor. de ~~[illegible]~~ LAGRANGE)

Soit G un groupe fini et $g \in G$. Alors

$$\mathrm{ord}_G(g) \text{ divise } |G|$$

Preuve : Il suffit d'appliquer le théorème de Lagrange au sous-groupe $\langle g \rangle \subset |G|$, car $|\langle g \rangle| = \mathrm{ord}_G(g)$.

Théorème (EULER)

Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ avec $\mathrm{PGCD}(a,n) = 1$.

Alors $$a^{\varphi(n)} \equiv 1 \mod n.$$

Preuve : On applique le théorème précédent au groupe des inversibles $G = (\mathbb{Z}/_{n\mathbb{Z}})^*$ et à l'élément $\bar{a} \in (\mathbb{Z}/_{n\mathbb{Z}})^*$ ($\bar{a}$ est inversible car $\mathrm{PGCD}(a,n) = 1$).

Donc, on obtient $\operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^*}(\bar{a})$ divise $\varphi(m)$

Donc, d'après une proposition précédente

$$\bar{a}^{\varphi(m)} = \bar{1} \quad \text{dans } (\mathbb{Z}/m\mathbb{Z})^*$$

$$\iff \quad a^{\varphi(m)} \equiv 1 \mod m \qquad \square$$

Corollaire (FERMAT)

Soit $a \in \mathbb{Z}$ et p premier. Si p ne divise pas a, alors .

$$a^{p-1} \equiv 1 \mod p.$$

<u>Preuve</u>: Si $m = p$ premier, alors $PGCD(a, p) = 1 \iff p$ ne divise pas m. De plus $\varphi(p) = p - 1$ (vu précédemment). $\square$

Retour sur les restes chinois

Résolution de systèmes de congruences

Soient $m_1, m_2, \dots, m_k$ des entiers 2 à 2 premiers entre eux.
et $a_1, \dots, a_k$ des entiers quelconques.

<u>Problème</u>: Trouver tous les entiers $x \in \mathbb{Z}$ vérifiant le système de k congruenes

$$(*) \quad \begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad \vdots \\ x \equiv a_k \mod m_k. \end{cases}$$

On sait qu'il existe un isomorphisme (restes chinois)

$$\Phi : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}).$$

Donc si $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$ est l'antécédent de $(\bar{a}_1, \dots, \bar{a}_k)$

c'est-à-dire $\Phi(\bar{y}) = (\bar{a}_1, \dots, \bar{a}_k)$

Alors $x \in \mathbb{Z}$ solution de $(*) \iff x \equiv y \mod n$.

(si $y \in \mathbb{Z}$ représentant de $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$).

__Question__ : Comment calculer l'antécédent $\bar{y}$?

. __Méthode générale__

On introduit $n = n_1 \cdot n_2 \cdots n_k = \prod_{i=1}^{k} n_i$

et $M_i = \dfrac{n}{n_i} = \prod_{\substack{j=1 \\ j \neq i}}^{k} n_j \iff n_i M_i = n$

Comme les n_i sont 2 à 2 premiers entre eux, on a $PGCD(M_i, n_i) = 1 \quad \forall i = 1, .., k$.

On peut donc considérer l'inverse de $M_i \bmod n_i$ noté y_i. C'est un entier vérifiant.

$$y_i M_i \equiv 1 \mod n_i$$

On pose

$$y = \sum_{j=1}^{k} a_j y_j M_j \pmod{n}.$$

__Rem__ : y est bien défini modulo n, car y_j est défini modulo n_j donc $y_j M_j$ est défini modulo. $n_j M_j = n$.

Il reste à vérifier que y est bien solution du système de congruences, c'est-à-dire que

$$y \equiv a_i \mod n_i$$

or
$$y = \sum_{\substack{j=1 \\ j \neq i}}^{k} a_j y_j M_j + a_i \underbrace{y_i M_i}_{\equiv 1 \mod n_i}$$

et $M_j \equiv 0 \mod n_i$ si $j \neq 0$.

$$\Rightarrow y \equiv a_i \mod n_i$$

- En pratique, il y a souvent des méthodes plus directes pour calculer y, p.ex. en testant certaines valeurs.

Remarque: Si les entiers $n_1, \dots, n_k$ ne sont pas 2 à 2 premiers entre eux, il peut arriver que le système n'a pas de solution.

p.ex. $\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 4 \end{cases}$ n'a pas de solution.