Arithmétique sur $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 1$ un entier. Rappelons que $(\mathbb{Z}/n\mathbb{Z})^*$ désigne le groupe des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Théorème : Soit a un entier. Alors $\bar{a}$ est inversible si et seulement si a et n sont premiers entre eux. Autrement dit, on a :

$$(\mathbb{Z}/n\mathbb{Z})^* = \{ \bar{a} \mid 1 \leq a \leq n \text{ et } \operatorname{pgcd}(a,n) = 1 \}$$

Preuve :

Supposons que $\bar{a}$ est inversible. Il existe alors $b \in \mathbb{Z}$ tel que $\bar{a}\bar{b} = \bar{1}$. Par suite, on a la congruence $ab \equiv 1 \mod 1$.

Autrement dit, il existe $c \in \mathbb{N}$ tel que $ab + cn = 1$

ce qui prouve que a et n sont premiers entre eux.

Inversement, d'après le théorème de Bézout, il existe des entiers u et v tels que l'on ait $au + nv = 1$. On obtient ainsi $\bar{a} \cdot \bar{u} = \bar{1}$, ce qui signifie que a est inversible.

Corollaire : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si p est premier.

Preuve : Supposons que $\mathbb{Z}/n\mathbb{Z}$ est un corps.
Soit q un diviseur positif de n. On a $n = qk$ où $k \in \mathbb{Z}$
d'où $\bar{n} = \bar{0} = \bar{q} \cdot \bar{k}$. Puisque $\mathbb{Z}/n\mathbb{Z}$ est un corps cela entraîne $\bar{q} = \bar{1}$
ou $\bar{k} = \bar{0}$. Ainsi n divise q auquel cas $q = n$ ou bien n divise k
auquel cas $k = n$ puisque $q = 1$. Cela prouve que n est premier.
Inversement, supposons que n soit premier. D'après le théorème précédent,
l'ordre de $(\mathbb{Z}/n\mathbb{Z})^*$ est alors $n-1$. Tous les éléments non-nuls de
$\mathbb{Z}/n\mathbb{Z}$ sont donc inversibles et $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Théorème d'Euler et petit théorème de Fermat

Définition (Fonction indicatrice d'Euler)
Pour tout entier $n \geq 1$, on définit l'entier $\varphi(n)$ comme étant le
nombre des entiers naturels plus petits que n et premiers avec n
Autrement dit :

$$\varphi(n) = \#\{ a \mid 1 \leq a \leq n,\ a \wedge n = 1 \} = \#(\mathbb{Z}/n\mathbb{Z})^*$$

Théorème (Euler) Soit $n \geq 1$ un entier. Pour un entier $a \in \mathbb{Z}$
premier avec n, on a la congruence

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

Preuve :

On sait que $\bar{a} \in ((\mathbb{Z}/n\mathbb{Z})^*, \times)$ qui est d'ordre $\varphi(n)$. D'après le théorème de Lagrange, on a donc dans $\mathbb{Z}/n\mathbb{Z}$ l'égalité

$$\bar{a}^{\varphi(n)} = \bar{1}$$

ce qui signifie que $a^{\varphi(n)} \equiv 1 \bmod n$.

Corollaire (Petit théorème de Fermat)

Soit p un nombre premier. Pour tout entier $a \in \mathbb{Z}$, non divisible par p, on a la congruence

$$a^{p-1} \equiv 1 \bmod p$$

En particulier, pour tout $a \in \mathbb{Z}$, on a $a^p \equiv a \bmod p$.

Preuve : Le théorème précédent entraîne l'assertion puisque $\varphi(p) = p - 1$. ∎

Exemple :

Posons $a = (1035125)^{5642}$. Déterminons le reste de la division euclidienne de a par 17. On a la congruence

$$1035125 \equiv 12 \bmod 17$$

D'après le petit théorème de Fermat, on a $12^{16} \equiv 1 \bmod 17$

Par ailleurs, on a $5642 \equiv 10 \bmod 16$.

On en déduit que l'on a $a \equiv 12^{5642} \equiv 12^{10} \bmod 17$.

On a $12 \equiv -5 \bmod 17$, $12^2 \equiv 8 \bmod 17$, $12^4 \equiv -4 \bmod 17$
$12^8 \equiv -1 \bmod 17$, d'où $a \equiv 9 \bmod 17$.

Théorème (Théorème Chinois)
Soient m et n deux entiers naturels non-nuls premiers entre eux. L'application

$$\Psi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

définie pour tout $a \in \mathbb{Z}$ par l'égalité :

$$\Psi(a) = (a+m\mathbb{Z}, a+n\mathbb{Z})$$

est un morphisme d'anneaux surjectif de noyau $mn\mathbb{Z}$.
En particulier, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes via l'application qui à tout élément $a+mn\mathbb{Z}$ de $\mathbb{Z}/mn\mathbb{Z}$ associe le couple $(a+m\mathbb{Z}, b+n\mathbb{Z})$ de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Preuve :
Notons que Ψ est bien un morphisme d'anneaux.
Vérifions que l'on a $\ker(\Psi) = mn\mathbb{Z}$.
Si $a \in \ker\Psi$, on a $(a+m\mathbb{Z}, b+n\mathbb{Z}) = (m\mathbb{Z}, n\mathbb{Z})$, autrement dit, $a \equiv 0 \bmod m$ et $b \equiv 0 \bmod n$. Puisque m et n sont premiers entre eux, on en déduit que mn divise a, i.e, $a \in mn\mathbb{Z}$.
Inversement, si a est dans $mn\mathbb{Z}$, alors a est évidemment

divisible par m et n donc $a \in \ker \Psi$.

Prouvons que Ψ est surjective. Considérons pour cela l'élément $(a+m\mathbb{Z}, b+n\mathbb{Z})$ de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Puisque m et n sont premiers entre eux, il existe deux entiers u et v tels que

$$mu + nv = 1$$

Posons alors $\quad c = b(mu) + a(nv)$

On vérifie qu'on a les congruences

$$\begin{aligned} c &\equiv a(nv) \mod m \\ &\equiv a(1-mu) \mod m \\ &\equiv a - amu \mod m \\ c &\equiv a \mod m \end{aligned}$$

De même, on a $\quad c \equiv b \mod n$. D'où

$$\Psi(c) = (a \mod m,\ b \mod n)$$

D'où Ψ est surjective.

Détermination de la fonction indicatrice d'Euler :

Théorème : Soit $n \geq 2$ un entier. On a l'égalité :

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

où p parcourt l'ensemble des diviseurs premiers de n.

Pour prouver ce théorème, on utilise le fait que la fonction φ est multiplicative, autrement dit :

Proposition : Soient m et n deux entiers naturels non nuls premiers entre eux. On a

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Preuve : Les entiers m et n étant premiers entre eux, les anneaux $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomorphes. Les groupes des éléments inversibles de ces éléments sont donc isomorphes. En particulier, ils ont le même cardinal. D'où

$$\begin{aligned}
\varphi(mn) &= \#(\mathbb{Z}/mn\mathbb{Z})^* \\
&= \#(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^* \\
&= \#((\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*) \\
&= \#(\mathbb{Z}/n\mathbb{Z})^* \cdot \#(\mathbb{Z}/m\mathbb{Z})^* \\
&= \varphi(n)\varphi(m)
\end{aligned}$$

■

Preuve du théorème :

Notons $p_1, \dots, p_r$ les diviseurs premiers de n.

Soit $$n = \prod_{i=1}^{r} p_i^{n_i}$$

la décomposition en facteurs premiers de n. On en déduit que :

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{n_i}).$$

Les entiers naturels plus petits que $p_i^{n_i}$ et premiers avec $p_i^{n_i}$ sont ceux qui sont plus petits que $p_i^{n_i}$ et qui ne sont pas multiples de p_i.
Comme il y a $\frac{p_i^{n_i}}{p_i} = p_i^{n_i-1}$ multiples de p_i compris entre 1 et $p_i^{n_i}$, on trouve que :

$$\varphi(p_i^{n_i}) = p_i^{n_i} - p_i^{n_i-1} = p_i^{n_i-1}(p_i-1)$$

Donc $$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{n_i}) = \prod_{i=1}^{r} p_i^{n_i-1}(p_i-1)$$

$$= \prod_{i=1}^{r} \left(p_i^{n_i}\left(1-\frac{1}{p_i}\right) \right)$$

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