# Théorie des nombres

Séance n°1, mardi 12 avril 2022

## Cours à retenir

Soit $n$ un entier supérieur ou égal à 2.

$\Phi(n)$ désigne le nombre d'entiers naturels inférieurs à $n$ et premiers avec $n$

<u>Propriétés</u>

Si $(m, n) = 1$ alors $\Phi(m \times n) = \Phi(m) \times \Phi(n)$

Si $p$ est un nombre premier alors $\Phi(p) = p - 1$ et $\Phi(p^k) = p^k - p^{k-1}$ , $k \in \mathbb{N}$

$\Phi(1) = 1$ et $\Phi(n) = n \prod_{p/n} \left(1 - \frac{1}{p}\right)$

Si $\mathrm{n} = \mathrm{p}_1{}^{\alpha_1} \mathrm{x} \mathrm{p}_2{}^{\alpha_2} \mathrm{x} \ldots \mathrm{x} \mathrm{p}_\mathrm{k}{}^{\alpha_\mathrm{k}}$ alors $\Phi(n) = \mathrm{n}\left(1 - \frac{1}{\mathrm{p}_1}\right) \mathrm{x} \left(1 - \frac{1}{\mathrm{p}_2}\right) \mathrm{x} \ldots \mathrm{x} \left(1 - \frac{1}{\mathrm{p}_\mathrm{k}}\right)$

<u>Théorème d'Euler</u>

Si $a$ et $n$ sont deux entiers premiers entre eux, alors $a^{\Phi(n)} \equiv 1 (mod n)$

<u>Petit théorème de Fermat</u>

En appliquant le théorème d'Euler pour $n = p$ où $p$ est un nombre premier, on obtient :

$$a^{\mathrm{p}} \equiv p (mod p)$$

Dans le cas $a$ et $n$ sont premiers entre eux, on obtient : $a^{\mathrm{p}-1} \equiv 1 (mod p)$

<u>Théorème de Wilson</u>

Un entier naturel $n \geq 2$ est premier, si et seulement si, $(n-1)! \equiv -1 \ (mod n)$.

## Problèmes

**Problème 1**

Trouver le reste de $3^{5^{11^{7!}}}$ dans la division par 19

**Problème 2**

Trouver le reste de 33! dans la division par 37.

**Problème 3**

Trouver toutes les fractions qui peuvent s'écrire à la fois sous la forme $\frac{7k-5}{5k-3}$ et $\frac{6l-1}{4l-3}$

**Problème 4**

Soit $a, b, c$ trois entiers naturels non nuls tel que $a$ divise $b^2$, $b$ divise $c^2$and $c$ divise $a^2$. Prouver que $abc$ divise $(a + b + c)^7$.

**Problème 5**

Trouver tous les entiers premiers $p$ tel que $\frac{2^{p-1}-1}{p}$ est un carré parfait

**Problème 6**

Montrer que si $2^m - 1$ est un nombre premier, alors $n = 2^{m-1}(2^m - 1)$ est un nombre parfait (Un entier $n$ est dit nombre parfait si l'entier $n$ est égal à la somme de ses diviseurs, sauf $n$ lui-même).