Scéance n°3. RSA

Exercice 1 *La fonction d'Euler*

Soit n un entier non nul. On a vu la fonction d'Euler φ qui donne le nombre $\varphi(n)$ d'entiers positifs plus petits que n et qui sont premiers avec n.

Rappelons que

- Si p est un nombre premier, alors $\varphi(p) = p - 1$.
- Si m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$ (i.e. φ est multiplicative).

1. Soit $n = 6 = 2 \times 3$.
   (a) Calculer $\varphi(6)$.
   (b) Vérifier que pour tout $x \in \mathbb{Z}$ tel que $\text{pgcd}(x, n) = 1$, on a $x^{\varphi(6)} \equiv 1\,[6]$.
   (Remarque : il suffit de travailler dans $\mathbb{Z}/6\mathbb{Z}$).
2. Même question avec $n = 15$.

On peut démontrer que de façon générale, si n est un entier positif, alors pour tout x tel que $\text{pgcd}(x, n) = 1$, on a $x^{\varphi(n)} \equiv 1\,[n]$.

$\star\star\star\star\star\star\star\star\star\star\star$

Exercice 2 *Application*

Posons $n = 35$.

1. Calculer $\varphi(35)$.
2. Soit $e = 5$. Montrer que e est inversible modulo $\varphi(35)$ et calculer son inverse d.
3. Montrer que pour tout $x \in \mathbb{Z}/35\mathbb{Z}$ telle que $\text{pgcd}(x, 35)$, on a
$$(x^e)^d = x^{ed} \equiv x\,[35]$$
(Ind. : utiliser le fait que $ed \equiv 1\,[35]$).
4. En théorie, on a donc une nouvelle fonction de codage : la fonction
$$\begin{array}{rccc} f & : & \mathbb{Z}/35\mathbb{Z} & \longrightarrow & \mathbb{Z}/35\mathbb{Z} \\ & & x & \longmapsto & x^e \end{array}$$
dont la fonction de décodage est la fonction
$$\begin{array}{rccc} f^{-1} & : & \mathbb{Z}/35\mathbb{Z} & \longrightarrow & \mathbb{Z}/35\mathbb{Z} \\ & & y & \longmapsto & y^d \end{array}$$
Quel problème rencontre-t-on si l'on veut mettre cette méthode en pratique ?

$\star\star\star\star\star\star\star\star\star\star\star$