09.01.23

## Théorème d'Euler

Si $pgdc(a,n) = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$

**Exemple :**

- $a = 28$ , $n = 15$ $\quad pgdc(28,15) = 1$
- $\varphi(15) = \varphi(3 \cdot 5) = (3-1)\cdot(5-1) = 2 \cdot 4 = 8$

$P = \{1, 2, 4, 7, 8, 11, 13, 14\}$ est l'ensemble des nombres premiers avec 15.

| | | | |
|---|---|---|---|
| $28 \cdot 1$ | $\equiv 28 \equiv$ | $13$ | $\pmod{15}$ |
| $28 \cdot 2$ | $\equiv 56 \equiv$ | $11$ | |
| $28 \cdot 4$ | $\equiv 112 \equiv$ | $7$ | |
| $28 \cdot 7$ | $\equiv 196 \equiv$ | $1$ | |
| $28 \cdot 8$ | $\equiv 224 \equiv$ | $14$ | |
| $28 \cdot 11$ | $\equiv 308 \equiv$ | $8$ | |
| $28 \cdot 13$ | $\equiv 364 \equiv$ | $4$ | |
| $28 \cdot 14$ | $\equiv 392 \equiv$ | $2$ | $\pmod{15}$ |

$(28\cdot1)\cdot(28\cdot2)\cdot(28\cdot4)\cdot(28\cdot7)\cdot(28\cdot8)\cdot(28\cdot11)\cdot(28\cdot13)\cdot(28\cdot14) \equiv (1\cdot2\cdot4\cdot7\cdot8\cdot11\cdot13\cdot14) \pmod{15}$

$$28^{8} \equiv 1 \pmod{15}$$

$$28^{\varphi(15)} \equiv 1 \pmod{15}$$

# Petit théorème de Fermat

Soit $p$ premier et $a \in \mathbb{N}$ avec $pgdc(a, p) = 1$. On a

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

## Corollaire

$$a^{p} \equiv a \pmod{p}$$

## Démonstration

$$a^{p} \equiv a \cdot \underbrace{a^{p-1}}_{1} \equiv a \pmod{p}$$

# Exemple de chiffrement RSA

1) Soit $p = 5$ et $q = 11$, $\boxed{n = 55}$ clé publique

2) $\varphi(55) = \varphi(5 \cdot 11) = \varphi(5)\,\varphi(11) = 4 \cdot 10 = 40$

3) Choisissons $e$ tq $pgdc(e, \varphi(n)) = pgdc(e, 40) = 1$, par exemple $\boxed{e = 7}$

4) Déterminons $\boxed{d}$ tel que $e\,d \equiv 1 \pmod{40}$ clé privée

Avec Bezout, on calcule $d$ :

$$7 \cdot d + 40 \cdot K = 1$$

| | | | | |
|---|---|---|---|---|
| 1 | 40 | 1 | 0 | |
| 2 | 7 | 0 | 1 | |
| 3 | 5 | 1 | -5 | $40 = 5 \cdot 7 + 5$ |
| 4 | 2 | -1 | 6 | $7 = 1 \cdot 5 + 2$ |
| 5 | 1 | 3 | -17 | $5 = 2 \cdot 2 + 1$ |

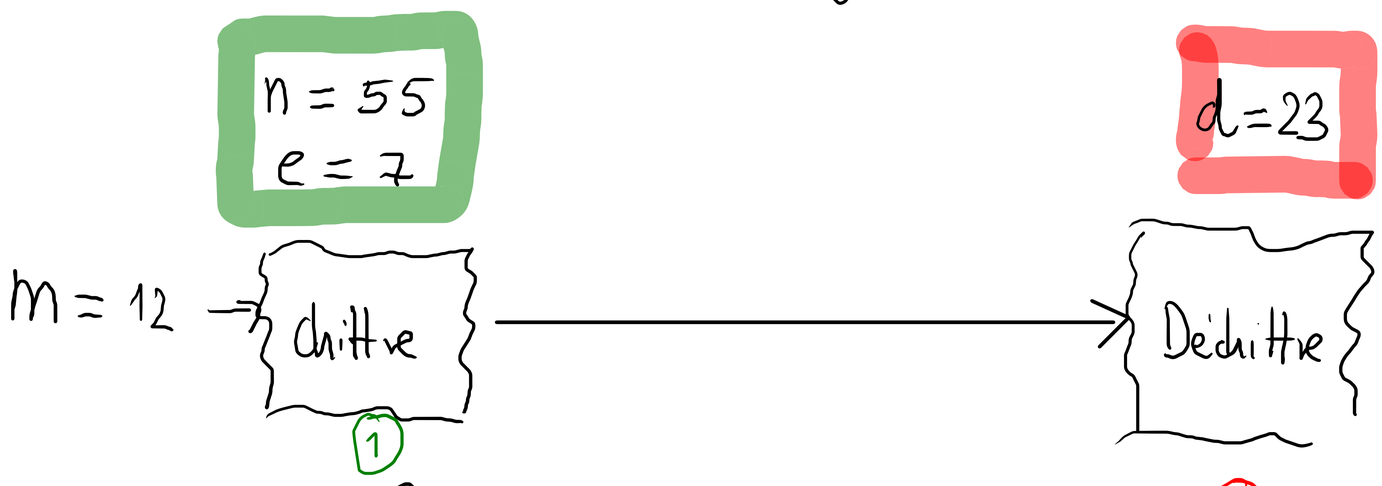
$$7 \cdot \underbrace{(-17)}_{d} + 40 \cdot 3 = 1$$

$$7 \cdot (-17) \equiv 1 \pmod{40}$$

On prend $d \equiv -17 \equiv 23 \pmod{40}$

$\boxed{d = 23}$

Nous devons chiffrer le message $m = 12$.




① $m^e \equiv 12^7 \equiv 23 \pmod{55}$

② $23^d \equiv 23^{23} \equiv 12 \pmod{55}$

Exemple 2

1) Alice choisit deux nombres premiers $p$ et $q$ qu'elle garde secret.

$p = 5$ et $q = 17$

2) Alice détermine la clé secrète et la clé publique.

clé publique : $e = 5$ et $n = 85$

clé privée : $d$ tel que $e \cdot d \equiv 1 \pmod{64}$

Algorithme d'Euclide étendu

| | | | | |
|---|---|---|---|---|
| 1 | 64 | 1 | 0 | |
| 2 | 5 | 0 | 1 | |
| 3 | 4 | 1 | −12 | $64 = 12 \cdot 5 + 4$ |
| 4 | 1 | −1 | 13 | $5 = 1 \cdot 4 + 1$ |

$d = 13$

3) Bob chiffre son message $X \equiv m^5 \pmod{85}$

4) Alice déchiffre le message $X^d \equiv (m^5)^{13} \equiv m^{5 \cdot 13} \equiv m \pmod{85}$

## Théorème (RSA)

Soit $p$ et $q$ deux nombres premiers distincts et $n = p \cdot q$.

Si $e$ est premier avec $\varphi(n)$ et $d$ est tel que $ed \equiv 1 \pmod{\varphi(n)}$

alors, pour tout entier $a$, on a $a^{ed} \equiv a \pmod{n}$

## Démonstration

Par le petit théorème de Fermat, on a $a^{p-1} \equiv 1 \pmod{p}$, $a \neq 0$

et donc pour tout $K \in \mathbb{N}$, on a $a^{K(p-1)} \equiv (a^{p-1})^K \equiv 1^K \equiv 1 \pmod{p}$

Ce qui implique que $a^{K(p-1)} \cdot a = a^{K(p-1)+1} \equiv a \pmod{p}$.

Comme $ed \equiv 1 \pmod{(p-1)(q-1)}$, il existe $k_1, k_2 \in \mathbb{Z}$ avec

$ed = k_1(p-1) + 1 = k_2(q-1) + 1$.

Donc $a^{ed} \equiv a \pmod{p}$ et $a^{ed} \equiv a \pmod{q}$

ou encore $a^{ed-1} \equiv 1 \pmod{p}$ et $a^{ed-1} \equiv 1 \pmod{q}$

Ce qui signifie qu'il existe $s$ et $t$ deux entiers tels que

$$a^{ed-1} - 1 = sp = tq$$

En vertu de l'unicité de la décomposition d'un nombre en facteurs premiers $p \mid t$ (et $q \mid s$)

Ainsi $t = Kp$, pour un certain $K$

$$\begin{aligned} a^{ed-1} - 1 &= tq \\ &= (K \cdot p)\, q \\ &= K \cdot pq \end{aligned}$$

et donc $a^{ed-1} \equiv 1 \pmod{pq}$ et $a^{ed} \equiv a \pmod{pq}$.