Cryptologie

Part 2

Bastien Vialla

bastien.vialla@orange.com

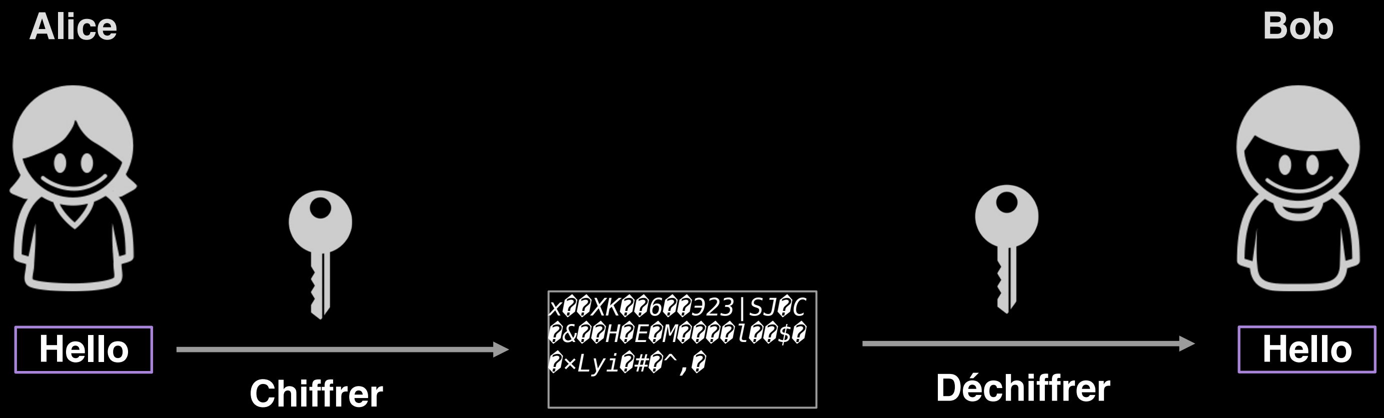
Année 2023-2024

Précédent cours

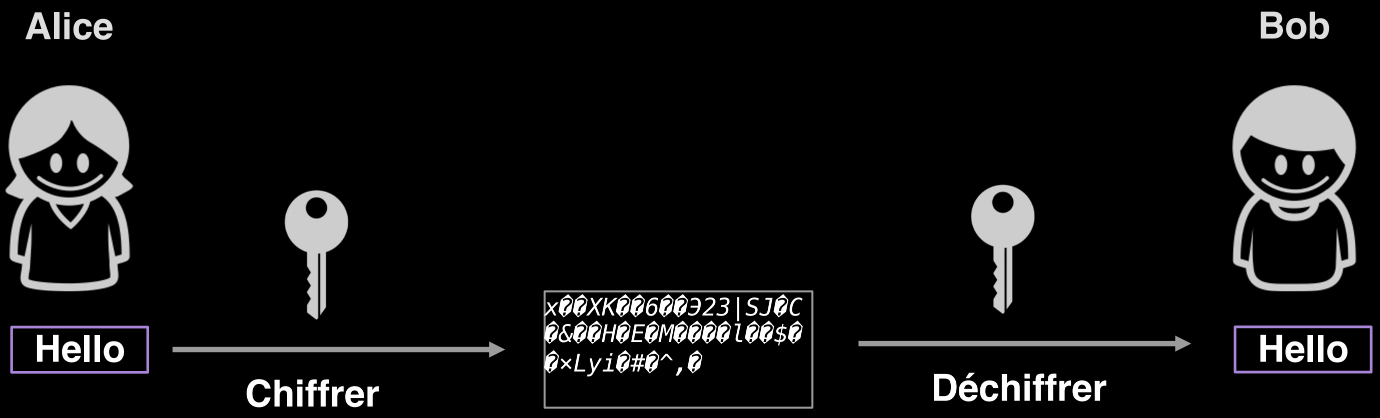
- **Définitions & vocabulaire**

- **Cryptographie symétrique:**
  - Chiffrement par permutation
  - Chiffrement par substitution monoalphabétique et polyalphabétique
  - Cryptanalyse
    - Analyse fréquentielle
    - Coefficient de coïncidence
  - Chiffrement par blocs
    - D.E.S

Cryptographie symétrique, ou à clé secrète

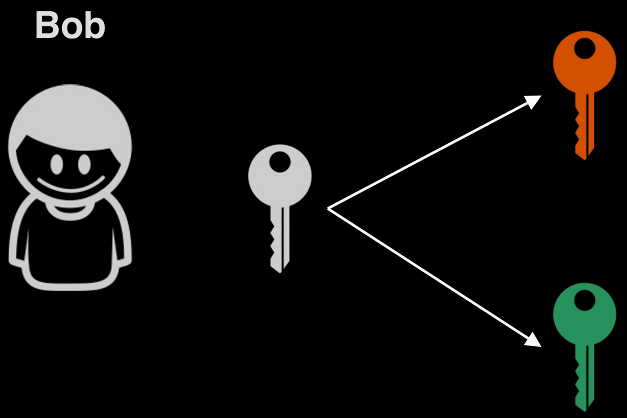


Cryptographie symétrique, ou à clé secrète

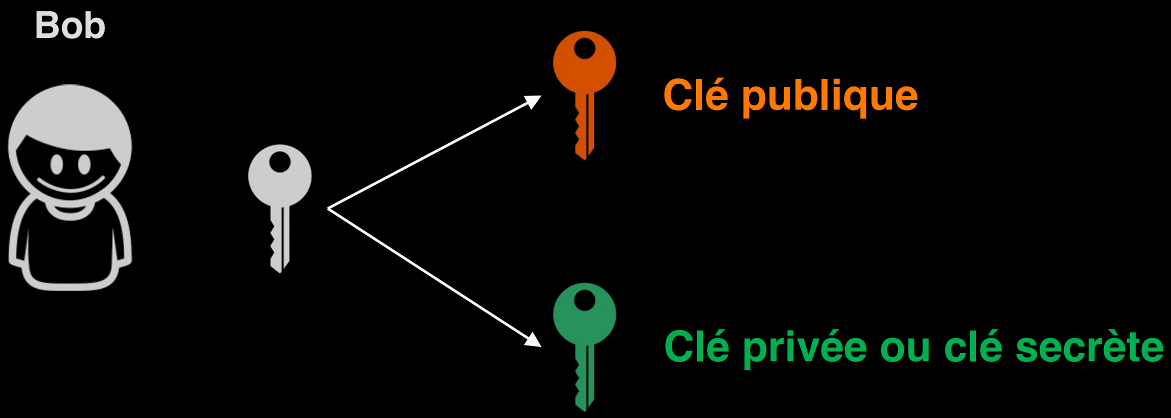


Inconvénient ?

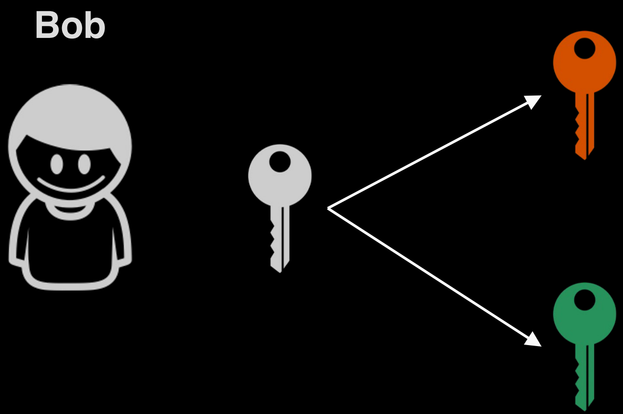
Cryptographie asymétrique, ou à clé publique



Cryptographie asymétrique, ou à clé publique



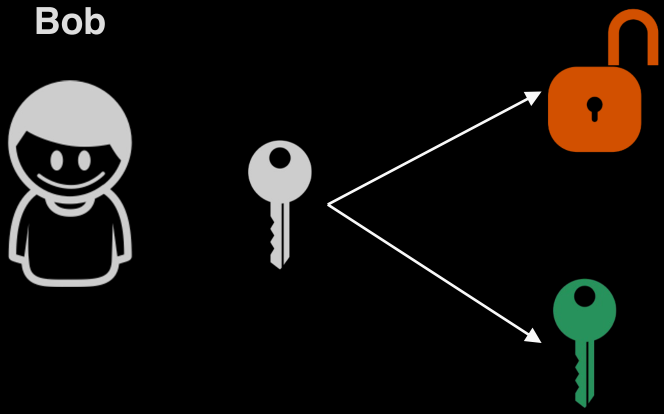
Cryptographie asymétrique, ou à clé publique



Clé publique : sert à chiffrer le message

Clé privée : sert à déchiffrer le message

Cryptographie asymétrique, ou à clé publique



Clé publique : sert à chiffrer le message

Clé privée : sert à déchiffrer le message

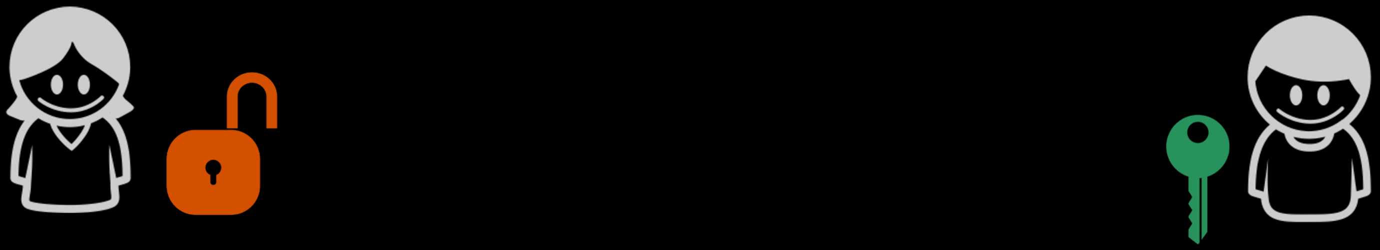
Cryptographie asymétrique, ou à clé publique

Alice

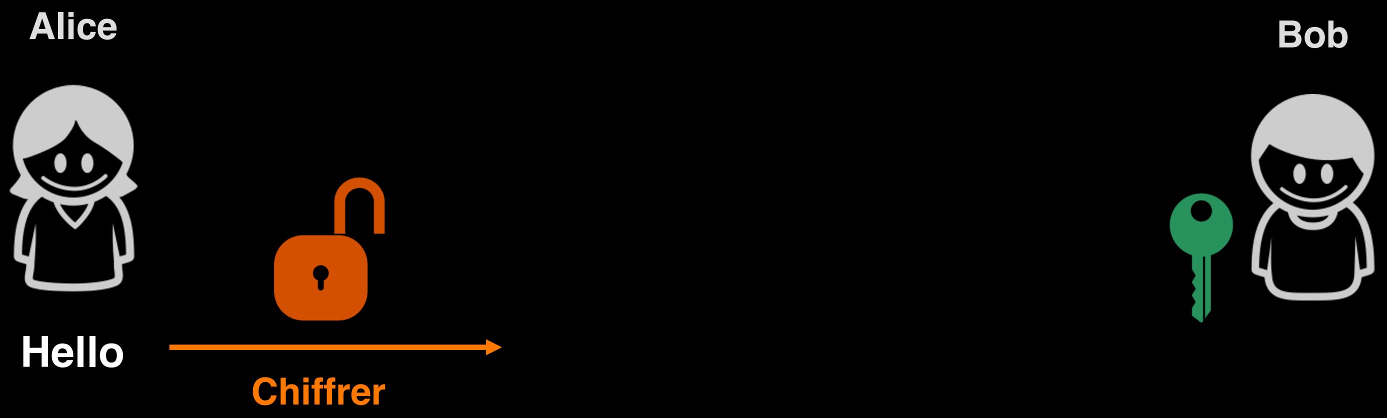
Hello

Bob

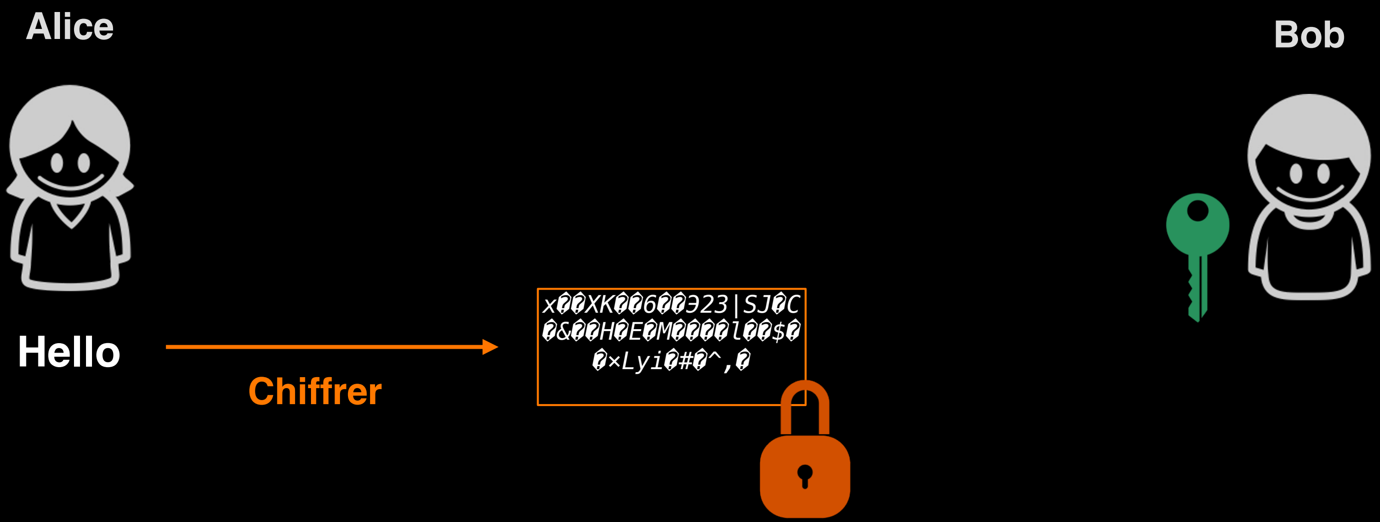
Cryptographie asymétrique, ou à clé publique



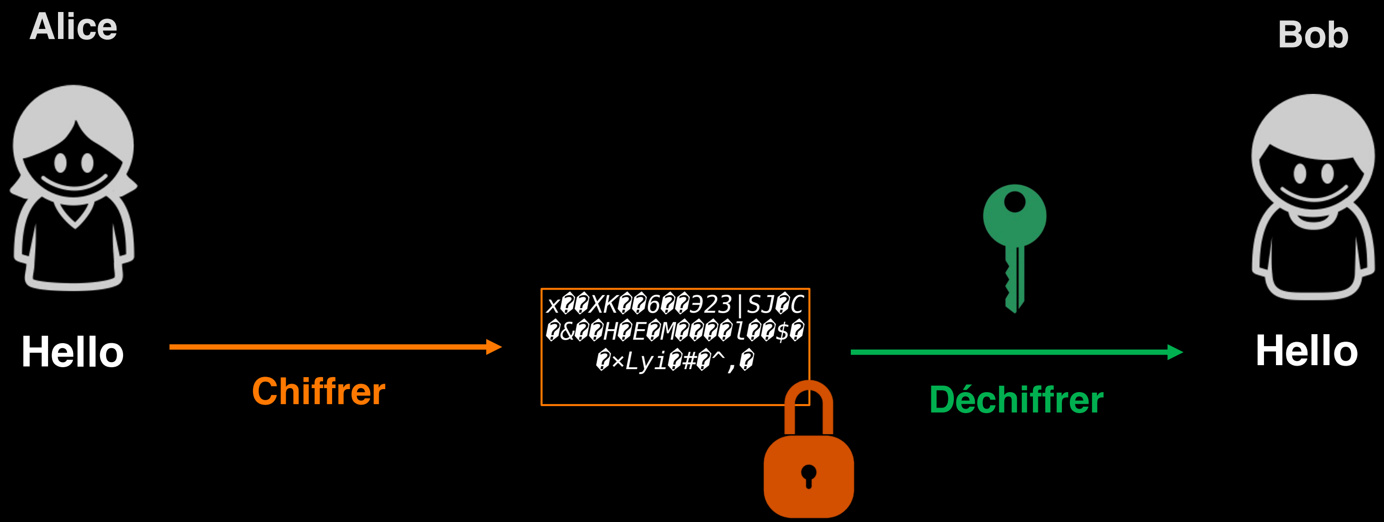
Cryptographie asymétrique, ou à clé publique



Cryptographie asymétrique, ou à clé publique



Cryptographie asymétrique, ou à clé publique



Cryptographie asymétrique, ou à clé publique

- **Une partie de la clé est maintenant connue de tous : la clé publique pk**

- **L’autre partie reste secrète : la clé secrète sk**

Cryptographie asymétrique, ou à clé publique

- Une partie de la clé est maintenant connue de tous : la clé publique pk

- L’autre partie reste secrète : la clé secrète sk

- Avantage : il n’y a plus besoin de partager un secret commun

Cryptographie asymétrique, ou à clé publique

- **Une partie de la clé est maintenant connue de tous : la clé publique pk**

- **L'autre partie reste secrète : la clé secrète sk**
- **Avantage : il n'y a plus besoin de partager un secret commun**
- **Important : il est difficile de retrouver sk à partir de pk**
- **Se base un problème mathématique difficile, fonction à trappe**
  - Difficile à inverser sans informations externes

Cryptographie asymétrique, ou à clé publique

- Une partie de la clé est maintenant connue de tous : la clé publique pk

- L’autre partie reste secrète : la clé secrète sk

- Avantage : il n’y a plus besoin de partager un secret commun
- Important : il est difficile de retrouver sk à partir de pk
- Se base un problème mathématique difficile, fonction à trappe
  - Difficile à inverser sans informations externes
- Exemple : R.S.A (factorisation d’entier), ElGamal (logarithme discret), …

Un peu de maths

Division euclidienne

Théorème:

Pour tout couple d'entiers (a,b) appartenant à $\mathbb{Z}\times\mathbb{Z}^*$, il existe un unique couple d'entiers (q,r) tel que

$$a = b.q + r \quad 0 \leq r \leq |b|$$

L'entier r (resp. q) est appelé le reste (resp. le quotient) de la division euclidienne de a par b.

Division euclidienne

Théorème:

Pour tout couple d'entiers (a,b) appartenant à $\mathbb{Z}\times\mathbb{Z}^*$, il existe un unique couple d'entiers (q,r) tel que

$$a = b.q + r \quad 0 \leq r \leq |b|$$

L'entier r (resp. q) est appelé le reste (resp. le quotient) de la division euclidienne de a par b.

- **Exemples :**

$$26 = 5 \cdot 5 + 1$$
$$31 = 3 \cdot 10 + 1$$
$$-52 = 6 \cdot (-7) - 3$$

Division euclidienne

Théorème:

Pour tout couple d'entiers (a,b) appartenant à $\mathbb{Z}\times\mathbb{Z}^*$, il existe un unique couple d'entiers (q,r) tel que

$$a = b.q + r \quad 0 \leq r \leq |b|$$

L'entier r (resp. q) est appelé le reste (resp. le quotient) de la division euclidienne de a par b.

- **Exemples :**

$$26 = 5 \cdot 5 + 1$$
$$31 = 3 \cdot 10 + 1$$
$$-52 = 6 \cdot (-7) - 3$$

```
q = a//b
r = a%b
```

Plus Grand Commun Diviseur (PGCD)

Définition:

Soient $a_1, \cdots, a_k$ des entiers relatifs ($\mathbb{Z}$). Le PGCD de $a_1, \cdots, a_k$ est le plus grand entier positif *d* divisant les $a_i, i = 1, \cdots, k$

Plus Grand Commun Diviseur (PGCD)

Définition:

Soient $a_1, \cdots, a_k$ des entiers relatifs ($\mathbb{Z}$). Le PGCD de $a_1, \cdots, a_k$ est le plus grand entier positif *d* divisant les $a_i, i = 1, \cdots, k$

- **Exemples :**

$$pgcd(8,2) = 2$$
$$pgcd(3,5) = 1$$
$$pgcd(3,6,9) = 3$$

Propriétés du PGCD

I. $pgcd(a_1, \cdots, a_k) = pgcd(a_1, d)\ avec\ d = pgcd(a_2, \cdots, a_k)$

II. $pgcd(a, b) = pgcd(|a|, |b|)$

Propriétés du PGCD

I. $pgcd(a_1, \cdots a_k) = pgcd(a_1, d)\ avec\ d = pgcd(a_2, \cdots, a_k)$

II. $pgcd(a, b) = pgcd(|a|, |b|)$

III. $pgcd(a, b) = pgcd(b, a)$ **le pgcd est commutatif**

IV. $pgcd(a, 0) = |a|$

Propriétés du PGCD

I. $pgcd(a_1, \cdots a_k) = pgcd(a_1, d)\ avec\ d = pgcd(a_2, \cdots, a_k)$

II. $pgcd(a, b) = pgcd(|a|, |b|)$

III. $pgcd(a, b) = pgcd(b, a)$ **le pgcd est commutatif**

IV. $pgcd(a, 0) = |a|$

V. **Si** $a = bq + r$ **est la division euclidienne de *a* par *b*, alors** $pgcd(a, b) = pgcd(b, r)$

Algorithme d'Euclide

Input : $a, b \in \mathbb{Z}$
Output : $pgcd(a, b)$

While $b \neq 0$ **do**

$\quad$ q, $r \longleftarrow Division(a, b)$
$\quad$ $a \longleftarrow b$
$\quad$ $b \longleftarrow r$

Return $|a|$

Complexité : $\mathcal{O}\left(\left(log_2(a) + log_2(b)\right)^2\right)$

Algorithme d'Euclide

Input : $a, b \in \mathbb{Z}$
Output : $pgcd(a, b)$

While $b \neq 0$ **do**

$q, r \longleftarrow Division(a, b)$
$a \longleftarrow b$
$b \longleftarrow r$

Return $|a|$

Complexité : $\mathcal{O}\left(\left(log_2(a) + log_2(b)\right)^2\right)$

Exemples :

I. $pgcd(68, 3) = 1$

$$68 = 3 \cdot 22 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

Algorithme d'Euclide

Input : $a, b \in \mathbb{Z}$
Output : $pgcd(a, b)$

While $b \neq 0$ **do**
$q, r \longleftarrow Division(a, b)$
$a \longleftarrow b$
$b \longleftarrow r$

Return $|a|$

Complexité : $\mathcal{O}\left(\left(log_2(a) + log_2(b)\right)^2\right)$

Exemples :

I. $pgcd(68, 3) = 1$

$$68 = 3 \cdot 22 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

II. $pgcd(112, 6) = 2$

$$112 = 6 \cdot 18 + 4$$
$$6 = 4 \cdot 1 + 2$$
$$4 = 2 \cdot 2 + 0$$

Coefficients de Bézout

Définition

Pour tout couple d'entiers *a* et *b*, il existe un couple d'entiers u et v, appelés coefficients de Bézout, et vérifiant

$$a \cdot u + b \cdot v = pgcd(a, b)$$

Coefficients de Bézout

Définition

Pour tout couple d'entiers *a* et *b*, il existe un couple d'entiers u et *v*, appelés coefficients de Bézout, et vérifiant

$$a \cdot u + b \cdot v = pgcd(a, b)$$

Exemples :

$$1 = 3 \cdot 23 + 68 \cdot (-1)$$
$$2 = 6 \cdot 19 + 112 \cdot (-1)$$
$$4 = 32 \cdot (-4) + 132 \cdot 1$$
$$5 = 35 \cdot (-3) + 55 \cdot 2$$

Coefficients de Bézout

Définition

Pour tout couple d'entiers *a* et *b*, il existe un couple d'entiers u et v, appelés coefficients de Bézout, et vérifiant

$$a \cdot u + b \cdot v = pgcd(a, b)$$

Exemples :

$$1 = 3 \cdot 23 + 68 \cdot (-1)$$
$$2 = 6 \cdot 19 + 112 \cdot (-1)$$
$$4 = 32 \cdot (-4) + 132 \cdot 1$$
$$5 = 35 \cdot (-3) + 55 \cdot 2$$

Attention ! Les coefficients ne sont pas uniques !

Algorithme d'Euclide étendu

Input : $a, b \in \mathbb{Z}$
Output : $pgcd(a,b)$ **et** u, v **tels que** $a \cdot u + b \cdot v = pgcd(a,b)$

$(u_0, u_1) \longleftarrow (1, 0)$
$(v_0, v_1) \longleftarrow (0, 1)$
While $b \neq 0$ **do**
  $\mathrm{q}, r \longleftarrow Division(a, b)$
  $(a, b) \longleftarrow (b, r)$
  $(\mathrm{u}_0, \mathrm{u}_1) \longleftarrow (u_1,\ u_0 - q \cdot u_1)$
  $(\mathrm{v}_0, \mathrm{v}_1) \longleftarrow (v_1,\ v_0 - q \cdot v_1)$

Return $|a|, u_0, v_0$

Algorithme d'Euclide étendu

Exemple : $a = 57, b = 33$
Init :
$(u_0, u_1) \longleftarrow (1,0)$
$(v_0, v_1) \longleftarrow (0,1)$

Etape 1 : $57 = 33 \times 1 + 24, \quad q = 1, \ r = 24$
$(a, b) \longleftarrow (33, 24)$
$(u_0, u_1) \longleftarrow (0, 1 - 1 \times 0) = (0, 1)$
$(v_0, v_1) \longleftarrow (1, 0 - 1 \times 1) = (1, -1)$

Algorithme d'Euclide étendu

Exemple : $a = 57, b = 33$

Init :

$(u_0, u_1) \longleftarrow (1{,}0)$

$(v_0, v_1) \longleftarrow (0, 1)$

Etape 1 : $57 = 33 \times 1 + 24, \quad q = 1, \ r = 24$

$(a, b) \longleftarrow (33, 24)$

$(u_0, u_1) \longleftarrow (0, 1 - 1 \times 0) = (0, 1)$

$(v_0, v_1) \longleftarrow (1, 0 - 1 \times 1) = (1, -1)$

Etape 2 : $33 = 24 \times 1 + 9, \quad q = 1, \ r = 9$

$(a, b) \longleftarrow (24, 9)$

$(u_0, u_1) \longleftarrow (1, 0 - 1 \times 1) = (1, -1)$

$(v_0, v_1) \longleftarrow (-1, 1 - 1 \times (-1)) = (-1, 2)$

Algorithme d'Euclide étendu

Exemple : $a = 57, b = 33$
Init :
$(u_0, u_1) \longleftarrow (1,0)$
$(v_0, v_1) \longleftarrow (0,1)$

Etape 1 : $57 = 33\times1 + 24, \quad q = 1,\ r = 24$
$(a, b) \longleftarrow (33, 24)$
$(u_0, u_1) \longleftarrow (0, 1 - 1\times0) = (0, 1)$
$(v_0, v_1) \longleftarrow (1, 0 - 1\times1) = (1, -1)$

Etape 2 : $33 = 24\times1 + 9, \quad q = 1,\ r = 9$
$(a, b) \longleftarrow (24, 9)$
$(u_0, u_1) \longleftarrow (1, 0 - 1\times1) = (1, -1)$
$(v_0, v_1) \longleftarrow (-1, 1 - 1\times(-1)) = (-1, 2)$

Etape 3 : $24 = 9\times2 + 6, \quad q = 2,\ r = 6$
$(a, b) \longleftarrow (9, 6)$
$(u_0, u_1) \longleftarrow \big(-1, 1 - 2\times(-1)\big) = (-1, 3)$
$(v_0, v_1) \longleftarrow (2, -1 - 2\times2) = (2, -5)$

Algorithme d'Euclide étendu

Exemple : $a = 57, b = 33$
Init :
$(u_0, u_1) \longleftarrow (1,0)$
$(v_0, v_1) \longleftarrow (0,1)$

Etape 1 : $57 = 33\times1 + 24, \quad q = 1,\ r = 24$
$(a, b) \longleftarrow (33, 24)$
$(u_0, u_1) \longleftarrow (0, 1 - 1\times0) = (0, 1)$
$(v_0, v_1) \longleftarrow (1, 0 - 1\times1) = (1, -1)$

Etape 2 : $33 = 24\times1 + 9, \quad q = 1,\ r = 9$
$(a, b) \longleftarrow (24, 9)$
$(u_0, u_1) \longleftarrow (1, 0 - 1\times1) = (1, -1)$
$(v_0, v_1) \longleftarrow (-1, 1 - 1\times(-1)) = (-1, 2)$

Etape 3 : $24 = 9\times2 + 6, \quad q = 2,\ r = 6$
$(a, b) \longleftarrow (9, 6)$
$(u_0, u_1) \longleftarrow \big(-1, 1 - 2\times(-1)\big) = (-1, 3)$
$(v_0, v_1) \longleftarrow (2, -1 - 2\times2) = (2, -5)$

Etape 4 : $9 = 6\times1 + 3, \quad q = 1,\ r = 3$
$(a, b) \longleftarrow (6, 3)$
$(u_0, u_1) \longleftarrow (3, -1 - 1\times3) = (3, -4)$
$(v_0, v_1) \longleftarrow \big(-5, 2 - 1\times(-5)\big) = (-5, 7)$

Algorithme d'Euclide étendu

Exemple : $a = 57, b = 33$
Init :
$(u_0, u_1) \longleftarrow (1,0)$
$(v_0, v_1) \longleftarrow (0,1)$

Etape 1 : $57 = 33\times1 + 24, \quad q = 1,\ r = 24$
$(a, b) \longleftarrow (33, 24)$
$(u_0, u_1) \longleftarrow (0, 1 - 1\times0) = (0, 1)$
$(v_0, v_1) \longleftarrow (1, 0 - 1\times1) = (1, -1)$

Etape 2 : $33 = 24\times1 + 9, \quad q = 1,\ r = 9$
$(a, b) \longleftarrow (24, 9)$
$(u_0, u_1) \longleftarrow (1, 0 - 1\times1) = (1, -1)$
$(v_0, v_1) \longleftarrow (-1, 1 - 1\times(-1)) = (-1, 2)$

Etape 3 : $24 = 9\times2 + 6, \quad q = 2,\ r = 6$
$(a, b) \longleftarrow (9, 6)$
$(u_0, u_1) \longleftarrow \big(-1, 1 - 2\times(-1)\big) = (-1, 3)$
$(v_0, v_1) \longleftarrow (2, -1 - 2\times2) = (2, -5)$

Etape 4 : $9 = 6\times1 + 3, \quad q = 1,\ r = 3$
$(a, b) \longleftarrow (6, 3)$
$(u_0, u_1) \longleftarrow (3, -1 - 1\times3) = (3, -4)$
$(v_0, v_1) \longleftarrow \big(-5, 2 - 1\times(-5)\big) = (-5, 7)$

Etape 5 : $6 = 3\times2 + 0, \quad q = 2,\ r = 0$
$(a, b) \longleftarrow (3, 0)$
$(u_0, u_1) \longleftarrow (-4, \cdots)$
$(v_0, v_1) \longleftarrow (7, \cdots)$

Algorithme d'Euclide étendu

Exemple : $a = 57, b = 33$
Init :
$(u_0, u_1) \longleftarrow (1{,}0)$
$(v_0, v_1) \longleftarrow (0, 1)$

Etape 1 : $57 = 33\times1 + 24, \quad q = 1,\ r = 24$
$(a, b) \longleftarrow (33, 24)$
$(u_0, u_1) \longleftarrow (0, 1 - 1\times0) = (0, 1)$
$(v_0, v_1) \longleftarrow (1, 0 - 1\times1) = (1, -1)$

Etape 2 : $33 = 24\times1 + 9, \quad q = 1,\ r = 9$
$(a, b) \longleftarrow (24, 9)$
$(u_0, u_1) \longleftarrow (1, 0 - 1\times1) = (1, -1)$
$(v_0, v_1) \longleftarrow (-1, 1 - 1\times(-1)) = (-1, 2)$

Etape 3 : $24 = 9\times2 + 6, \quad q = 2,\ r = 6$
$(a, b) \longleftarrow (9, 6)$
$(u_0, u_1) \longleftarrow \big(-1, 1 - 2\times(-1)\big) = (-1, 3)$
$(v_0, v_1) \longleftarrow (2, -1 - 2\times2) = (2, -5)$

Etape 4 : $9 = 6\times1 + 3, \quad q = 1,\ r = 3$
$(a, b) \longleftarrow (6, 3)$
$(u_0, u_1) \longleftarrow (3, -1 - 1\times3) = (3, -4)$
$(v_0, v_1) \longleftarrow \big(-5, 2 - 1\times(-5)\big) = (-5, 7)$

Etape 5 : $6 = 3\times2 + 0, \quad q = 2,\ r = 0$
$(a, b) \longleftarrow (3, 0)$
$(u_0, u_1) \longleftarrow (-4, \cdots)$
$(v_0, v_1) \longleftarrow (7, \cdots)$

Résultat : $57 \times (-4) + \ 33 \times 7 = 3$

Algorithme d'Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1		
9	1		
6	2		
3	1		
0	2		

Algorithme d’Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1	$1 - 1 \times 0 = 1$	
9	1		
6	2		
3	1		
0	2		

Algorithme d'Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1	1	
9	1	$0 - 1 \times 1 = -1$	
6	2		
3	1		
0	2		

Algorithme d’Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1	1	
9	1	-1	
6	2	$1 - 2\times(-1) = 3$	
3	1		
0	2		

Algorithme d’Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1	1	
9	1	-1	
6	2	3	
3	1	$-1 - 1 \times 3 = -4$	
0	2		

Algorithme d’Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1	1	
9	1	-1	
6	2	3	
3	1	-4	
0	2		

Algorithme d'Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1	1	$0 - 1 \times 1 = -1$
9	1	-1	
6	2	3	
3	1	-4	
0	2		

Algorithme d'Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1	1	-1
9	1	-1	2
6	2	3	-5
3	1	-4	$2 - 1 \times (-5) = 7$
0	2		

Algorithme d'Euclide étendu

r	q	u	v
$a = 57$		1	0
$b = 33$		0	1
24	1	1	-1
9	1	-1	2
6	2	3	-5
3	1	-4	7
0	2		

Algorithme d'Euclide étendu

$\boldsymbol{r}$	$\boldsymbol{q}$	$\boldsymbol{u}$	$\boldsymbol{v}$
$a = 57$		1	0
$b = 33$		0	1
24	1	1	-1
9	1	-1	2
6	2	3	-5
3	1	-4	7
0	2		

$$57 \times (-4) + 33 \times 7 = 3$$

Algorithme d'Euclide étendu

$$\begin{pmatrix} u_0 & u_1 \\ v_0 & v_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} u_1 & u_0 - q \cdot u_1 \\ v_1 & v_0 - q \cdot v_1 \end{pmatrix}$$

Algorithme d'Euclide étendu

r	q
$a = 57$	
$b = 33$	
24	1
9	1
6	2
3	1
0	2

$$\begin{pmatrix} u_0 & u_1 \\ v_0 & v_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} u_1 & u_0 - q \cdot u_1 \\ v_1 & v_0 - q \cdot v_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

Algorithme d'Euclide étendu

$\boldsymbol{r}$	$\boldsymbol{q}$
$a = 57$	
$b = 33$	
24	1
9	1
6	2
3	1
0	2

$$\begin{pmatrix} u_0 & u_1 \\ v_0 & v_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} u_1 & u_0 - q \cdot u_1 \\ v_1 & v_0 - q \cdot v_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

Algorithme d’Euclide étendu

r	q
$a = 57$	
$b = 33$	
24	1
9	1
6	2
3	1
0	2

$$\begin{pmatrix} u_0 & u_1 \\ v_0 & v_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} u_1 & u_0 - q \cdot u_1 \\ v_1 & v_0 - q \cdot v_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

Algorithme d'Euclide étendu

$\boldsymbol{r}$	$\boldsymbol{q}$
$a = 57$	
$b = 33$	
24	1
9	1
6	2
3	1
0	2

$$\begin{pmatrix} u_0 & u_1 \\ v_0 & v_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} u_1 & u_0 - q \cdot u_1 \\ v_1 & v_0 - q \cdot v_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} -1 & -3 \\ 3 & -5 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

Algorithme d'Euclide étendu

r	q
$a = 57$	
$b = 33$	
24	1
9	1
6	2
3	1
0	2

$$\begin{pmatrix} u_0 & u_1 \\ v_0 & v_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} u_1 & u_0 - q \cdot u_1 \\ v_1 & v_0 - q \cdot v_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} -1 & -3 \\ 3 & -5 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 3 & -4 \\ -5 & 7 \end{pmatrix}$$

Algorithme d'Euclide étendu

r	q
$a = 57$	
$b = 33$	
24	1
9	1
6	2
3	1
0	2

$$\begin{pmatrix} u_0 & u_1 \\ v_0 & v_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} = \begin{pmatrix} u_1 & u_0 - q \cdot u_1 \\ v_1 & v_0 - q \cdot v_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} -1 & -3 \\ 3 & -5 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} 3 & -4 \\ -5 & 7 \end{pmatrix}$$

$$57 \times (-4) + 33 \times 7 = 3$$

Arithmétique modulaire

Définition :

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}, n > 1$. Soient q et r le quotient et le reste de la division euclidienne de a par n, i.e., $a = q \cdot n + r$. On dit que a est congrue à r modulo n. On le note

$$a \equiv r \bmod n \qquad (a = r \bmod n)$$

On appelle n le modulus.

Arithmétique modulaire

Définition :

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}, n > 1$. Soient q et r le quotient et le reste de la division euclidienne de a par n, i.e., $a = q \cdot n + r$. On dit que a est congrue à r modulo n. On le note

$$a \equiv r \bmod n \qquad (a = r \bmod n)$$

On appelle n le modulus.

Définition :

Soient $r \in \mathbb{Z}$ et $n \in \mathbb{N}, n > 1$. On appelle classe résiduelle de r modulo n, noté $\bar{r}$, l'ensemble :

$$\{r + n\mathbb{Z}\} = \{r + q \cdot n, q \in \mathbb{Z}\} = \{\cdots, r - 2 \cdot n, r - 1 \cdot n, r, r + 1 \cdot n, r + 2 \cdot n, \cdots\}$$

Arithmétique modulaire

Définition :

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}, n > 1$. Soient q et r le quotient et le reste de la division euclidienne de a par n, i.e., $a = q \cdot n + r$. On dit que a est congrue à r modulo n. On le note

$$a \equiv r \bmod n \qquad (a = r \bmod n)$$

On appelle n le modulus.

Définition :

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}, n > 1$. On appelle classe résiduelle de a modulo n, noté $\bar{a}$, l'ensemble :

$$\{a + n\mathbb{Z}\} = \{a + q \cdot n, q \in \mathbb{Z}\} = \{\cdots, a - 2 \cdot n, a - 1 \cdot n, a, a + 1 \cdot n, a + 2 \cdot n, \cdots\}$$

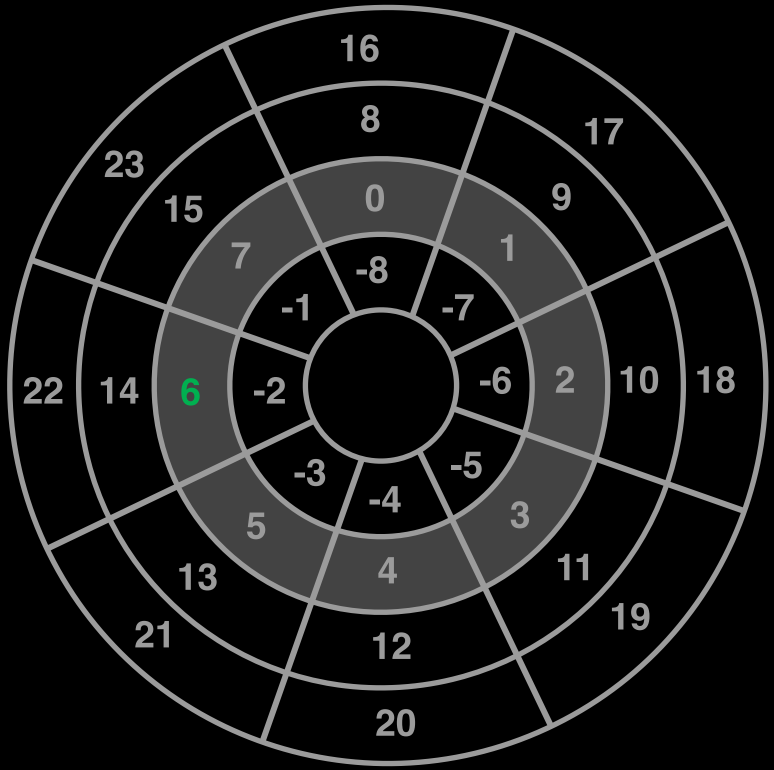
Définition :

Soit $n \in \mathbb{N}, n > 1$. L'ensemble des représentants des classes résiduelles modulo n, $\{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$ est noté

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

Arithmétique modulaire modulo 8

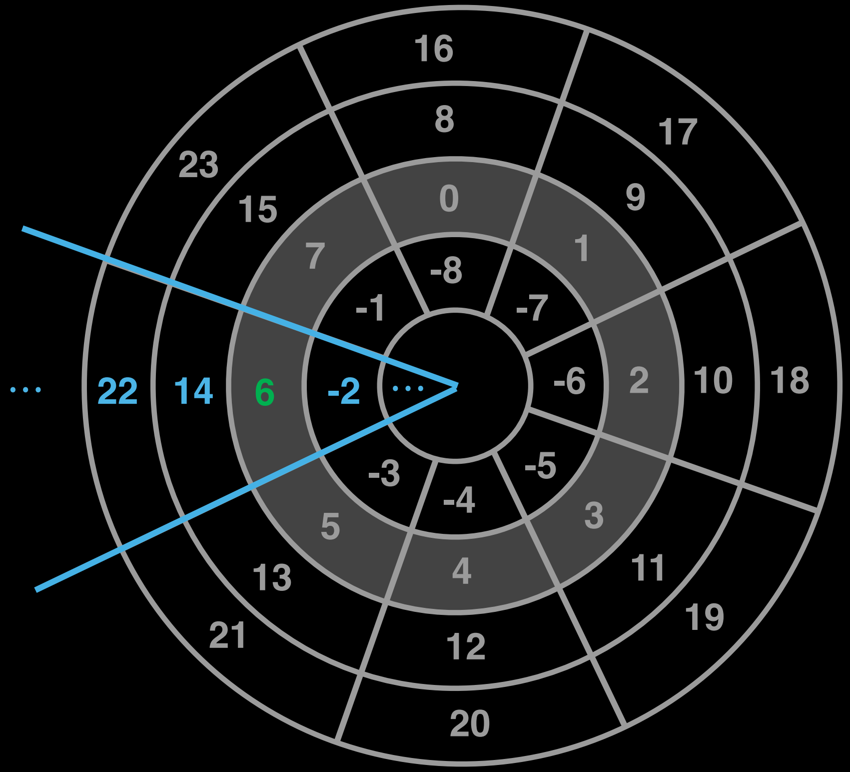
- **Classe résiduelle de 6 modulo 8**



Arithmétique modulaire modulo 8

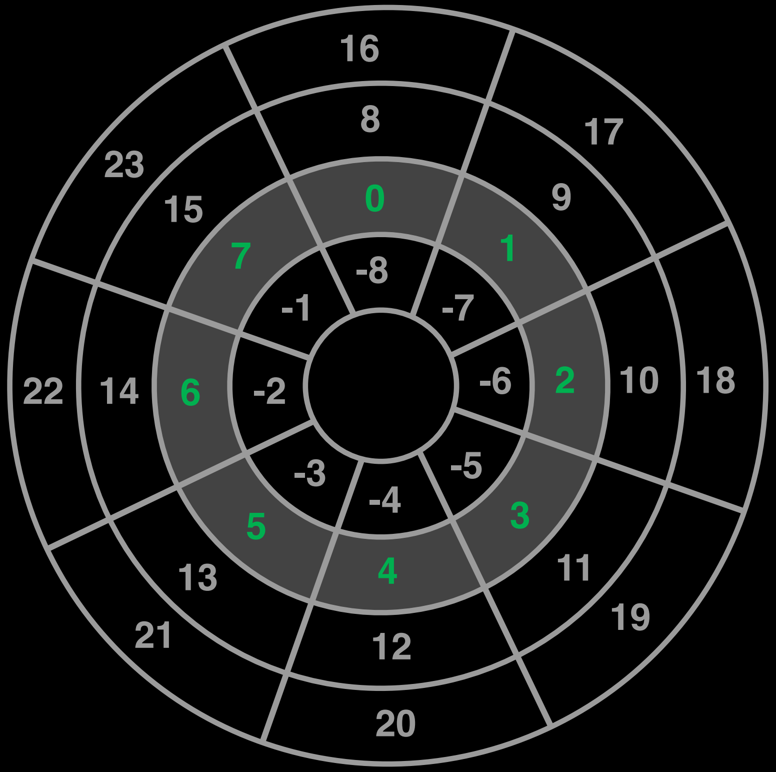
- **Classe résiduelle de 6 modulo 8**

$$\{\cdots, 6-2\times 8, 6-8, 6, 6+8, 6+2\times 8, \cdots\}$$
$$=$$
$$\{\cdots, -10, -2, 6, 14, 22, \cdots\}$$



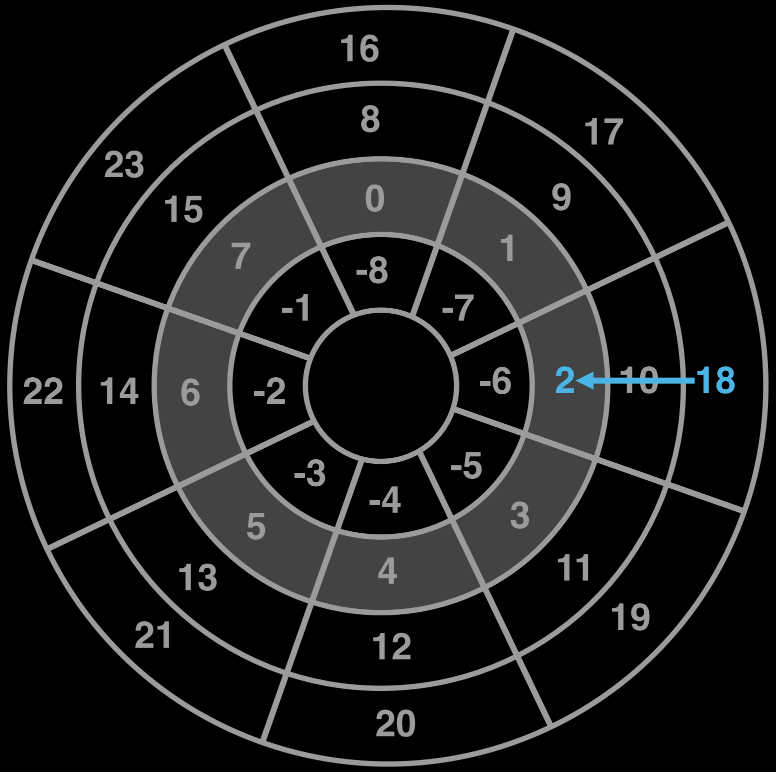
Arithmétique modulaire modulo 8

- **Classe résiduelle de 6 modulo 8**
- $\mathbb{Z}/8\mathbb{Z}$ **est l'ensemble** $\{0, 1, 2, 3, 4, 5, 6, 7\}$



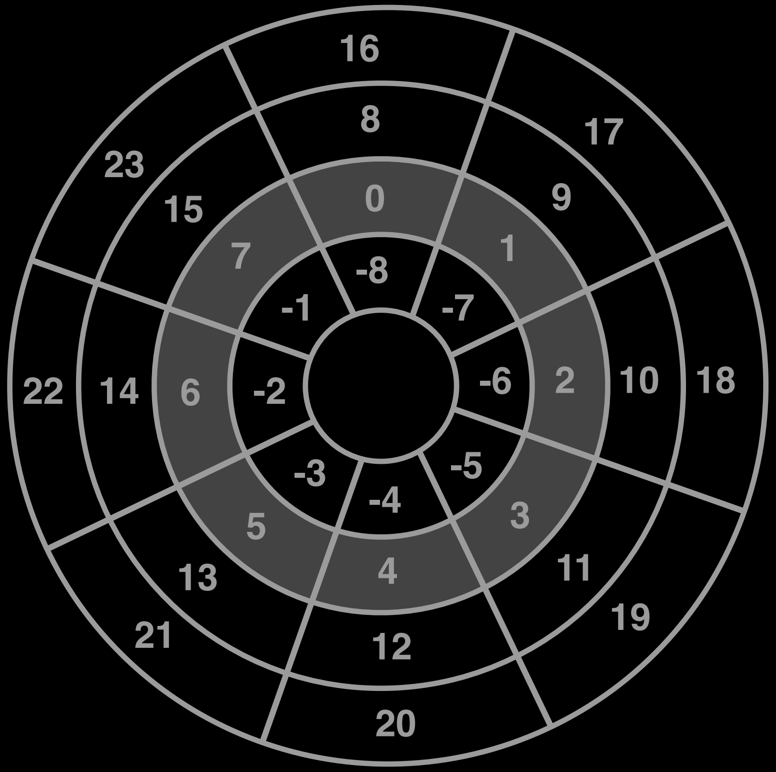
Arithmétique modulaire modulo 8

- $18 = 2{\times}8 + 2 \quad \longrightarrow 18 \equiv 2 \bmod 8$



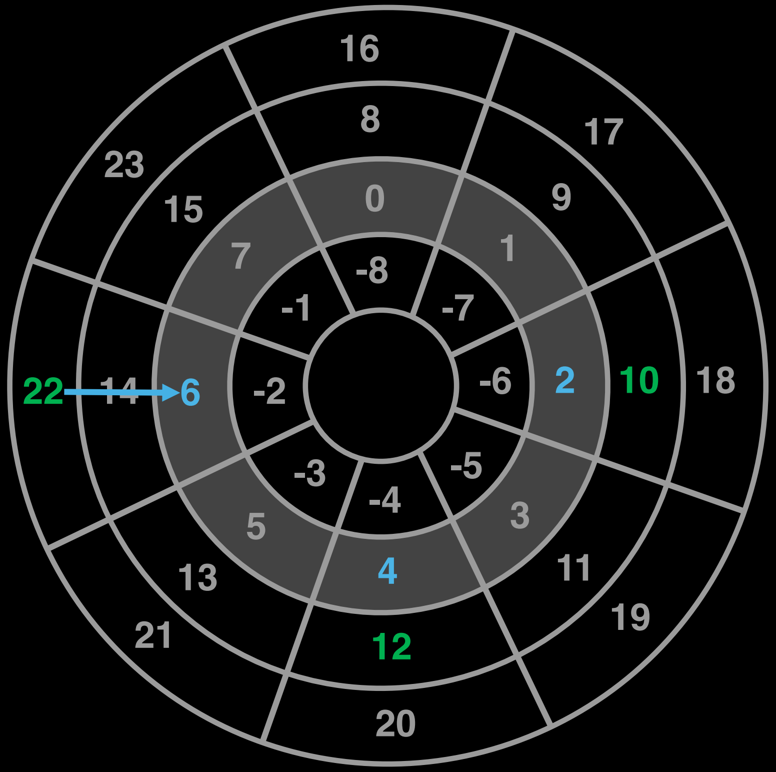
Arithmétique modulaire modulo 8

- $18 = 2{\times}8 + 2 \;\longrightarrow 18 \equiv 2 \bmod 8$
- **Addition** $a_1 + a_2 \equiv b_1 + b_2 \bmod n$



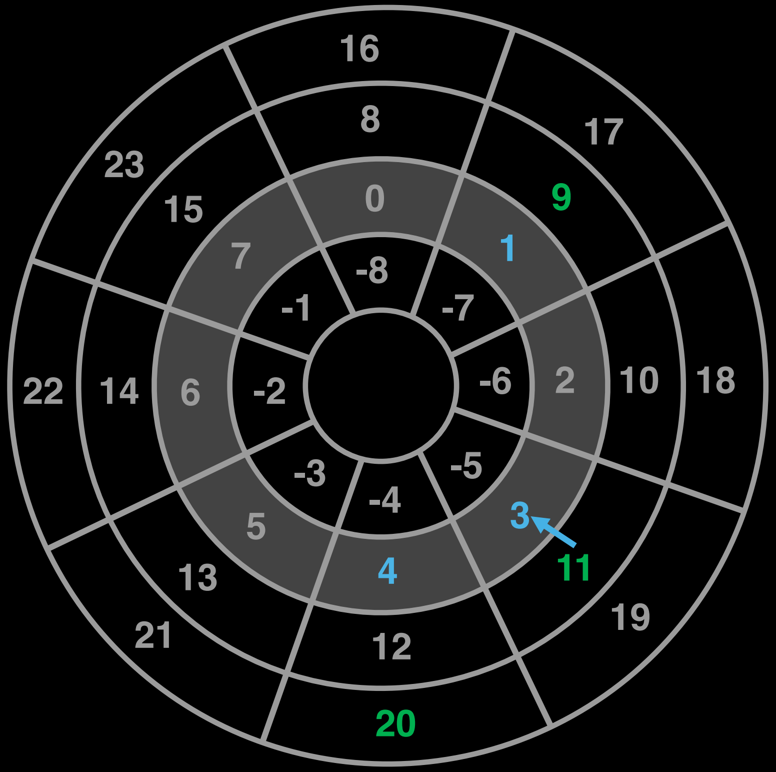
Arithmétique modulaire modulo 8

- $18 = 2{\times}8 + 2 \;\longrightarrow 18 \equiv 2 \bmod 8$
- **Addition** $a_1 + a_2 \equiv b_1 + b_2 \bmod n$
  - $10 + 12 \equiv 2 + 4 \bmod 8 = 6$



Arithmétique modulaire modulo 8

- $18 = 2{\times}8 + 2 \quad \longrightarrow 18 \equiv 2 \bmod 8$
- **Addition** $a_1 + a_2 \equiv b_1 + b_2 \bmod n$
- **Soustraction** $a_1 - a_2 \equiv b_1 - b_2 \bmod n$
  - $20 - 9 \equiv 4 - 1 \bmod 8 = 3$

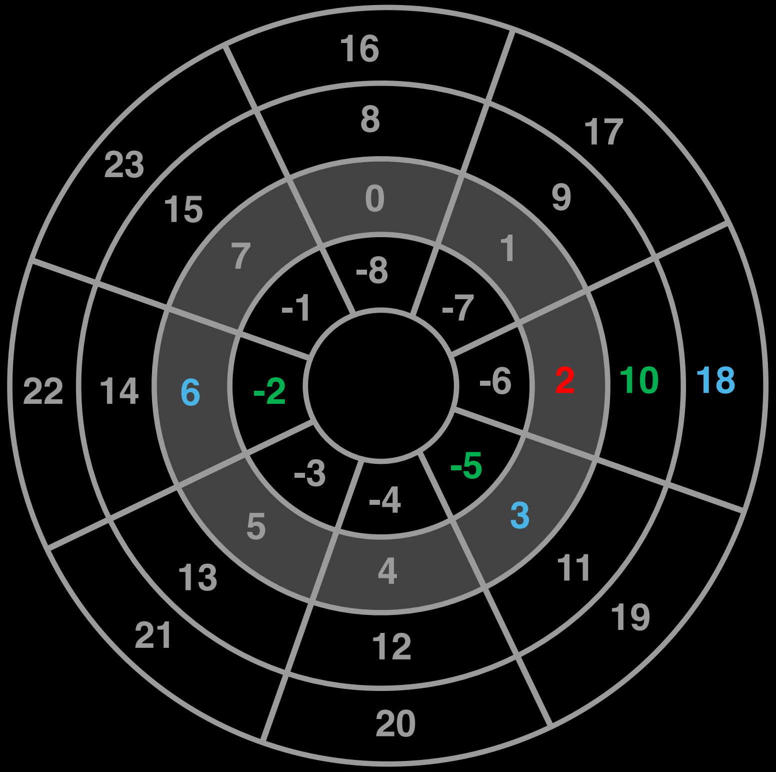


Arithmétique modulaire modulo 8

- $18 = 2\times 8 + 2 \quad \longrightarrow 18 \equiv 2 \bmod 8$
- **Addition** $a_1 + a_2 \equiv b_1 + b_2 \bmod n$
- **Soustraction** $a_1 - a_2 \equiv b_1 - b_2 \bmod n$
  - $20 - 9 \equiv 4 - 1 \bmod 8 = 3$
  - $9 - 12 \equiv 1 - 4 \bmod 8 \equiv -3 \bmod 8 = 5$

Arithmétique modulaire modulo 8

- $18 = 2{\times}8 + 2 \quad \longrightarrow 18 \equiv 2 \bmod 8$
- **Addition** $a_1 + a_2 \equiv b_1 + b_2 \bmod n$
- **Soustraction** $a_1 - a_2 \equiv b_1 - b_2 \bmod n$
- **Multiplication** $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \bmod n$
  - $-2{\times}-5 \equiv 3{\times}6\ mod\ 8 = 18 \equiv 2\ mod\ 8$



Inverse modulaire

Définition :

Un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible s'il existe un élément $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \cdot y = 1$

Inverse modulaire

Définition :

Un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible s'il existe un élément $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \cdot y = 1$

Exemples :

$$6 \times 2 = 12 \equiv 1 \bmod 11 \quad \Longrightarrow \quad 6^{-1} \bmod 11 = 2, \quad 2^{-1} \bmod 11 = 6$$

$$9 \times 5 = 45 \equiv 1 \bmod 11 \quad \Longrightarrow \quad 9^{-1} \bmod 11 = 5, \quad 5^{-1} \bmod 11 = 9$$

Inverse modulaire

Définition :

Un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible s'il existe un élément $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \cdot y = 1$

Exemples :

$$6 \times 2 = 12 \equiv 1 \bmod 11 \quad \Longrightarrow \; 6^{-1} \bmod 11 = 2, \quad 2^{-1} \bmod 11 = 6$$

$$9 \times 5 = 45 \equiv 1 \bmod 11 \quad \Longrightarrow \; 9^{-1} \bmod 11 = 5, \quad 5^{-1} \bmod 11 = 9$$

Comment calculer l'inverse ?

Inverse modulaire

Définition :

Un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible s'il existe un élément $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \cdot y = 1$

Exemples :

$$6 \times 2 = 12 \equiv 1 \bmod 11 \quad \Longrightarrow \quad 6^{-1} \bmod 11 = 2, \quad 2^{-1} \bmod 11 = 6$$

$$9 \times 5 = 45 \equiv 1 \bmod 11 \quad \Longrightarrow \quad 9^{-1} \bmod 11 = 5, \quad 5^{-1} \bmod 11 = 9$$

Comment calculer l'inverse ?

$$6 \times 2 \equiv 1 \bmod 11 \quad \Longrightarrow \quad \exists q \text{ tel que } 6 \times 2 + q \times 11 = 1$$

Inverse modulaire

Définition :

Un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible s'il existe un élément $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \cdot y = 1$

Calcul de l'inverse :

$$x \cdot y \equiv 1 \bmod n \implies \exists q \text{ tel que } \underbrace{x \cdot y + q \cdot n = 1}_{\textbf{Identité de Bézout}}$$

Inverse modulaire

Définition :

Un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible s'il existe un élément $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x \cdot y = 1$

Calcul de l'inverse :

$$x \cdot y \equiv 1 \bmod n \quad \Longrightarrow \quad \exists q \text{ tel que } \underbrace{x \cdot y + q \cdot n = 1}_{\textbf{Identité de Bézout}}$$

y, q **sont les coefficients de Bézout de** x **et** n**. On utilise l'algorithme d'Euclide étendu.**

Nombres premiers

Nombres premiers

Définition et théorème :

Deux entier *a* et *b* sont premiers entre eux si $pgcd(a, b) = 1$. Deux entiers a et b sont premiers entre eux si et seulement si il existe deux entiers *u* et *v* tels que

$$a \cdot u + b \cdot v = 1$$

Nombres premiers

Définition et théorème :

Deux entier *a* et *b* sont premiers entre eux si $pgcd(a,b) = 1$. Deux entiers a et b sont premiers entre eux si et seulement si il existe deux entiers *u* et *v* tels que

$$a \cdot u + b \cdot v = 1$$

Définition :

Un entier n est dit premier si et seulement si

1. $n \geq 2$
2. n n'est divisible que par $1, -1, n, -n$

Nombres premiers

Définition et théorème :

Deux entier *a* et *b* sont premiers entre eux si $pgcd(a, b) = 1$. Deux entiers a et b sont premiers entre eux si et seulement si il existe deux entiers *u* et *v* tels que

$$a \cdot u + b \cdot v = 1$$

Définition :

Un entier n est dit premier si et seulement si

1. $n \geq 2$
2. n n'est divisible que par $1, -1, n, -n$

Exemple : $2, 3, 5, 7, 11, 13, 17, 19, \cdots$

Nombres premiers

Définition et théorème :

Deux entier *a* et *b* sont premiers entre eux si $pgcd(a, b) = 1$. Deux entiers a et b sont premiers entre eux si et seulement si il existe deux entiers *u* et *v* tels que

$$a \cdot u + b \cdot v = 1$$

Définition :

Un entier n est dit premier si et seulement si

1. $n \geq 2$
2. n n'est divisible que par $1, -1, n, -n$

Exemple : $2, 3, 5, 7, 11, 13, 17, 19, \cdots$

Attention ! Les nombres pairs (sauf 2) ne sont pas premiers !

Quelques propriétés

Théorème :

Il existe une infinité de nombres premiers.

Quelques propriétés

Théorème :

Il existe une infinité de nombres premiers.

Proposition :

Si p est un nombre premier qui divise le produit $a \cdot b$ alors p divise a ou b

Quelques propriétés

Théorème :

Il existe une infinité de nombres premiers.

Proposition :

Si p est un nombre premier qui divise le produit $a \cdot b$ alors p divise a ou b

Théorème :

Soient a, b, c trois entiers tels que $a|bc$. Si a est premier avec b, alors a divise c.

Quelques propriétés

Théorème :

Il existe une infinité de nombres premiers.

Proposition :

Si p est un nombre premier qui divise le produit $a \cdot b$ alors p divise a ou b

Théorème :

Soient a, b, c trois entiers tels que $a|bc$. Si a est premier avec b, alors a divise c.

Théorème:

Tout nombre entier positif et ≥ 2 peut s'écrire sous la forme d'un produit fini de puissances de nombres premiers, la décomposition est unique à l'ordre près des facteurs premiers.

Génération de nombres premiers

- **Pour construire un nombre premier de taille fixée**
  - On tire au hasard un nombre et on teste sa primalité

Génération de nombres premiers

- **Pour construire un nombre premier de taille fixée**
  - On tire au hasard un nombre et on teste sa primalité

- **Tests de primalité**
  1. Divisions successives
     - Déterministe, lent pour de grands nombres

Génération de nombres premiers

- **Pour construire un nombre premier de taille fixée**
  - On tire au hasard un nombre et on teste sa primalité

- **Tests de primalité**
  1. Divisions successives
     - Déterministe, lent pour de grands nombres
  2. Petit théorème de Fermat
     - Test probabiliste, échoue avec les nombres Carmichael
  3. Test Miller-Rabin
     - Test probabiliste, utilisé dans la pratique

Génération de nombres premiers

- **Pour construire un nombre premier de taille fixée**
  - On tire au hasard un nombre et on teste sa primalité

- **Tests de primalité**

1. Divisions successives
   - Déterministe, lent pour de grands nombres
2. Petit théorème de Fermat
   - Test probabiliste, échoue avec les nombres Carmichael
3. Test Miller-Rabin
   - Test probabiliste, utilisé dans la pratique
4. Test AKS
   - Test déterministe, complexité polynomiale, pas utilisé en pratique
5. Test sur courbes elliptiques:
   - Test déterministe, utile pour des entiers $> 2^{10^5}$

Génération de nombres premiers

- **Pour construire un nombre premier de taille fixée**
  - On tire au hasard un nombre et on teste sa primalité

- **Tests de primalité**
  1. Divisions successives
     - Déterministe, lent pour de grands nombres
  2. Petit théorème de Fermat
     - Test probabiliste, échoue avec les nombres Carmichael
  3. Test Miller-Rabin
     - Test probabiliste, utilisé dans la pratique
  4. Test AKS
     - Test déterministe, complexité polynomiale, pas utilisé en pratique
  5. Test sur courbes elliptiques:
     - Test déterministe, utile pour des entiers $> 2^{10^5}$

Test primalité : divisions successives

- On teste si aucun des nombres $< \sqrt{n}$ divisent n

Test primalité : divisions successives

- On teste si aucun des nombres $< \sqrt{n}$ divisent n

```python
def is_prime(n):
    if n < 2:
        return False
    if n <= 3:
        return True
    if n % 2 == 0 or n % 3 == 0:
        return False
    i = 5
    while i * i <= n:
        if n % i == 0 or n % (i + 2) == 0:
            return False
        i += 6
    return True
```

Test primalité : Petit théorème de Fermat

Théorème:

Soit p un entier premier et $a \in \mathbb{Z}$ tel que $pgcd(a, p) = 1$. Alors

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

Test primalité : Petit théorème de Fermat

Théorème:

Soit p un entier premier et $a \in \mathbb{Z}$ tel que $pgcd(a, p) = 1$. Alors

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

Attention ! Le test de Fermat donne une condition nécessaire mais pas suffisante.

Test primalité : Petit théorème de Fermat

Théorème:

Soit p un entier premier et $a \in \mathbb{Z}$ tel que $pgcd(a, p) = 1$. Alors

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

Attention ! Le test de Fermat donne une condition nécessaire mais pas suffisante.

$$n \text{ premier } \Longrightarrow a^{n-1} \equiv 1 \bmod n$$

Test primalité : Petit théorème de Fermat

Théorème:

Soit p un entier premier et $a \in \mathbb{Z}$ tel que $pgcd(a,p) = 1$. Alors

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

Attention ! **Le test de Fermat donne une condition nécessaire mais pas suffisante.**

$$n \text{ premier } \Longrightarrow a^{n-1} \equiv 1 \bmod n \qquad\qquad a^{n-1} \equiv 1 \bmod n \not\Longrightarrow n \text{ premier}$$

Test primalité : Petit théorème de Fermat

Théorème:

Soit p un entier premier et $a \in \mathbb{Z}$ tel que $pgcd(a, p) = 1$. Alors

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

Attention ! Le test de Fermat donne une condition nécessaire mais pas suffisante.

$$n \text{ premier } \Longrightarrow a^{n-1} \equiv 1 \bmod n \qquad\qquad a^{n-1} \equiv 1 \bmod n \cancel{\Longrightarrow} n \text{ premier}$$

$$a^{n-1} \not\equiv 1 \bmod n \Longrightarrow n \text{ non premier}$$

Test primalité : Petit théorème de Fermat

Input : $n \in \mathbb{N}$, un entier k
Output : True si *n* est probablement premier, False si *n* n'est pas premier

For i in 0 … k
  Choisir aléatoirement $a < n, a \in \mathbb{N}$
  Calculer $s = a^{n-1} \bmod n$
  If $s \neq 1$
    Return False
Return True

Test primalité : Petit théorème de Fermat

Input : $n \in \mathbb{N}$, un entier k
Output : True si *n* est probablement premier, False si *n* n'est pas premier

For i in 0 … k
    Choisir aléatoirement $a < n, a \in \mathbb{N}$
    Calculer $s = a^{n-1} \bmod n$
    If $s \neq 1$
        Return False
Return True

- **La probabilité de retourner** True **si** n **est composé :** $\frac{1}{2^k}$

Test primalité : Petit théorème de Fermat

Input : $n \in \mathbb{N}$, un entier k
Output : True si *n* est probablement premier, False si *n* n'est pas premier

For i in 0 … k
  Choisir aléatoirement $a < n, a \in \mathbb{N}$
  Calculer $s = a^{n-1} \bmod n$
  If $s \neq 1$
    Return False
Return True

- **La probabilité de retourner** True **si** n **est composé :** $\frac{1}{2^k}$

- **Exemple :** $n = 341, a = 2 \longrightarrow 2^{340} \equiv 1 \bmod 341$

Test primalité : Petit théorème de Fermat

Input : $n \in \mathbb{N}$**,** un entier k
Output : True si *n* est probablement premier, False si *n* n'est pas premier

For i in 0 … k
 Choisir aléatoirement $a < n, a \in \mathbb{N}$
 Calculer $s = a^{n-1} \bmod n$
 If $s \neq 1$
  Return False
Return True

- **La probabilité de retourner** True **si** n **est composé :** $\frac{1}{2^k}$

- **Exemple :** $n = 341, a = 2 \longrightarrow 2^{340} = 1 \bmod 341$**, or** $341 = 13 \times 11$

Petit théorème de Fermat (version forte)

Théorème:

Soit n un entier impair. On écrit $n-1=2^k q$ avec q impair. Quelque soit b tel que $pgcd(n,b)=1$, si n est premier alors on a une des deux conditions suivantes:

1. $b^q \equiv 1 \bmod n$
2. $b^{2^i q} \equiv -1 \bmod n$ pour $0 \leq i \leq k-1$

Petit théorème de Fermat (version forte)

Théorème:

Soit n un entier impair. On écrit $n-1=2^k q$ avec q impair. Quelque soit b tel que $pgcd(n,b)=1$, si n est premier alors on a une des deux conditions suivantes:

1. $b^q \equiv 1 \bmod n$
2. $b^{2^i q} \equiv -1 \bmod n$ pour $0 \leq i \leq k-1$

Si $b^q \equiv 1 \bmod n$ ou il existe $i \in [0, k-1]$ tel que $b^{2^i q} \equiv -1 \bmod n$ $\Longrightarrow$ n est probablement premier

Si $b^q \not\equiv 1 \bmod n$ et pour tout $i \in [0, k-1]$ tel que $b^{2^i q} \not\equiv -1 \bmod n$ $\Longrightarrow$ n est composé

Test Miller Rabin

Input : $n \in \mathbb{N}$ impair
Output : True si *n* est probablement premier, False si *n* n'est pas premier

1. Calculer k et q tels que $n - 1 = 2^k q$ avec q impair
2. Choisir b aléatoirement dans $]1, \cdots, n-1[$ tel que $pgcd(b, n) = 1$
3. $x \longleftarrow b^q \bmod n$
4. **If** $x == 1$ **or** $x == n - 1$: **Return** True
4. **For** i **in** $1 \cdots k - 1$:
5. | $x \longleftarrow x^2 \bmod n$
6. | **If** $x == n - 1$**: Return** True
7. **Return** False

Test Miller Rabin

Input : $n \in \mathbb{N}$ impair
Output : True si *n* est probablement premier, False si *n* n'est pas premier

1. Calculer k et q tels que $n - 1 = 2^k q$ avec q impair
2. Choisir b aléatoirement dans $]1, \cdots, n-1[$ tel que $pgcd(b, n) = 1$
3. $x \longleftarrow b^q \bmod n$
4. **If** $x == 1$ **or** $x == n - 1$: **Return** True
4. **For** i **in** $1 \cdots k - 1$:
5. | $x \longleftarrow x^2 \bmod n$
6. | **If** $x == n - 1$**: Return** True
7. **Return** False

- **C'est un algorithme de Monté-Carlo, biaisé vers le faux**
- **La probabilité de faux positifs de l'algorithme est** $< \frac{1}{4^k}$

Test Miller Rabin : exemple

1. Calculer k et q tels que $n-1=2^k q$ avec q impair
2. Choisir b aléatoirement dans $]1,\cdots,n-1[$ tel que $pgcd(b,n)=1$
3. $x \longleftarrow b^q \bmod n$
4. **If** $x == 1$ **or** $x == n-1$: **Return** True
4. **For** i **in** $1 \cdots k-1$:
5. $\quad x \longleftarrow x^2 \bmod n$
6. $\quad$ **If** $x == n-1$**: Return** True
7. **Return** False

Input : $n = 221 = 13\times 17$

1. $n-1 = 220 = 2^2\times 55 \;\longrightarrow k=2, q=55$
2. $b = 137$
3. $x \longleftarrow 137^{55} \bmod 221 = 188$
4. $x \neq 1, x \neq 220$
5. $x \longleftarrow 188^2 \bmod 221 = 205$
6. $205 \neq 220$
7. **Return** False

- **La probabilité de faux positifs de l'algorithme est** $< \frac{1}{4^k} = \frac{1}{16}$

Test Miller Rabin : exemple

1. Calculer k et q tels que $n-1=2^k q$ avec q impair
2. Choisir b aléatoirement dans $]1,\cdots,n-1[$ tel que $pgcd(b,n)=1$
3. $x \longleftarrow b^q \bmod n$
4. **If** $x == 1$ **or** $x == n-1$: **Return** True
4. **For** i **in** $1 \cdots k-1$:
5. $\quad x \longleftarrow x^2 \bmod n$
6. $\quad$ **If** $x == n-1$**: Return** True
7. **Return** False

Input : $n = 221 = 13{\times}17$

1. $n-1 = 220 = 2^2{\times}55 \ \longrightarrow k=2, q=55$
2. $b = 174$
3. $x \longleftarrow 174^{55} \bmod 221 = 47$
4. $x \neq 1, x \neq 220$
5. $x \longleftarrow 47^2 \bmod 221 = 220$
6. $x = 220$
7. **Return** True

- **La probabilité de faux positifs de l'algorithme est** $< \frac{1}{4^k} = \frac{1}{16}$

Test Miller Rabin

Input : $n \in \mathbb{N}$ impair
Output : True si *n* est probablement premier, False si *n* n'est pas premier

1. Calculer k et q tels que $n - 1 = 2^k q$ avec q impair
2. Choisir b aléatoirement dans $]1, \cdots n-1[$ tel que $pgcd(b, n) = 1$
3. $x \longleftarrow b^q \bmod n$
4. **If** $x == 1$ **or** $x == n - 1$: **Return** True
4. **For** i **in** $1 \cdots k - 1$:
5. $\quad x \longleftarrow x^2 \bmod n$
6. $\quad$ **If** $x == n - 1$: **Return** True
7. **Return** False

- **C'est un algorithme de Monté-Carlo, biaisé vers le faux**
- **La probabilité de faux positifs de l'algorithme est** $< \frac{1}{4^k}$
- **On peut améliorer la probabilité d'être sûr du résultat, en essayant plusieurs** b

Indicatrice d'Euler

Définition:

Soit n un entier. Le nombre de nombres premiers avec n compris entre 1 et $n-1$ est noté $\phi(n)$. La fonction ϕ s 'appelle l'indicatrice d'Euler.

- **Plus formellement,** $\phi(n) = \#\{a \in \{1, \cdots, n-1\} \mid pgcd(a, n) = 1\}$

Indicatrice d'Euler

Définition:

Soit n un entier. Le nombre de nombres premiers avec n compris entre 1 et $n-1$ est noté $\phi(n)$. La fonction ϕ s 'appelle l'indicatrice d'Euler.

- **Plus formellement,** $\phi(n) = \#\{a \in \{1, \cdots, n-1\} \mid pgcd(a,n) = 1\}$
- **Si** p **est premier, alors** $\phi(p) = p - 1$

Indicatrice d’Euler

Définition:

Soit n un entier. Le nombre de nombres premiers avec n compris entre 1 et $n-1$ est noté $\phi(n)$. La fonction ϕ s ’appelle l’indicatrice d’Euler.

- **Plus formellement,** $\phi(n) = \#\{a \in \{1, \cdots, n-1\} \mid pgcd(a,n) = 1\}$
- **Si** p **est premier, alors** $\phi(p) = p - 1$
- **Si** p **est premier et** α **un entier positif, alors**

$$\phi(p^\alpha) = (p-1) \cdot p^{\alpha-1} = p^\alpha - p^{\alpha-1}$$

Indicatrice d'Euler

Définition:

Soit n un entier. Le nombre de nombres premiers avec n compris entre 1 et $n-1$ est noté $\phi(n)$. La fonction ϕ s 'appelle l'indicatrice d'Euler.

- **Plus formellement,** $\phi(n) = \#\{a \in \{1, \cdots, n-1\} \mid pgcd(a,n) = 1\}$
- **Si** p **est premier, alors** $\phi(p) = p - 1$
- **Si** p **est premier et** α **un entier positif, alors**

$$\phi(p^\alpha) = (p-1) \cdot p^{\alpha-1} = p^\alpha - p^{\alpha-1}$$

- **Si la décomposition en facteurs de** n **est donnée par** $n = {p_1}^{k_1}{p_2}^{k_2} \cdots {p_l}^{k_l}$**, alors**

$$\phi(n) = \phi\left({p_1}^{k_1}\right) \cdots \phi\left({p_l}^{k_l}\right) = (p_1 - 1){p_1}^{k_1-1} \cdots (p_l - 1){p_l}^{k_l-1}$$

Indicatrice d'Euler : exemples

$$\phi(2) = 1$$

$$\phi(5) = 4$$

$$\phi(8) = \phi(2^3) = (2-1) \cdot 2^{3-1} = 4$$

$$\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$$

$$\phi(144) = \phi(16 \cdot 9) = \phi(2^4 \cdot 3^2) = (2-1) \cdot 2^3 \cdot (3-1) \cdot 3 = 8 \cdot 2 \cdot 3 = 48$$

Théorème d'Euler et de Fermat

Théorème d'Euler:

Soit n un entier et x tel que $pgcd(x, n) = 1$. Alors

$$x^{\phi(n)} \equiv 1 \bmod n$$

Théorème d'Euler et de Fermat

Théorème d'Euler:

Soit n un entier et x tel que $pgcd(x, n) = 1$. Alors

$$x^{\phi(n)} \equiv 1 \bmod n$$

Théorème de Fermat:

Soit p un entier premier et x tel que $pgcd(x, n) = 1$. Alors

$$x^{\phi(p)} = x^{p-1} \equiv 1 \bmod p$$

Schéma R.S.A (Rivest, Shamir, Adleman)

R.S.A

- **Génération des clés :**
  1. Soit p et q deux grands premiers (1024 bits)
  2. Soit $N = p \cdot q$ (2048 bits)

R.S.A

- **Génération des clés :**
  1. Soit p et q deux grands premiers (1024 bits)
  2. Soit $N = p \cdot q$ (2048 bits)
  3. Soient e, d deux entiers premiers avec $\phi(N) = (p-1) \cdot (q-1)$ et $ed \equiv 1 \bmod \phi(N)$
  4. Finalement
     - Clé publique (pk) : (N, e)
     - Clé secrète (sk) : (d, p, q)

R.S.A

- **Génération des clés :**
  1. Soit p et q deux grands premiers (1024 bits)
  2. Soit $N = p \cdot q$ (2048 bits)
  3. Soient e, d deux entiers premiers avec $\phi(N) = (p-1) \cdot (q-1)$ et $ed \equiv 1 \, mod \, \phi(N)$
  4. Finalement
     - Clé publique (pk) : (N, e)
     - Clé secrète (sk) : (d, p, q)

- **Chiffrer : message** $m \in \mathbb{Z}/N\mathbb{Z}$

$$c \equiv m^e \bmod N$$

R.S.A

- **Génération des clés :**
  1. Soit p et q deux grands premiers (1024 bits)
  2. Soit $N = p \cdot q$ (2048 bits)
  3. Soient e, d deux entiers premiers avec $\phi(N) = (p-1) \cdot (q-1)$ et $ed \equiv 1 \bmod \phi(N)$
  4. Finalement
     - Clé publique (pk) : (N, e)
     - Clé secrète (sk) : (d, p, q)

- **Chiffrer : message** $m \in \mathbb{Z}/N\mathbb{Z}$

$$c \equiv m^e \bmod N$$

- **Déchiffrer :**

$$m \equiv c^d \bmod N$$

R.S.A

- **Déchiffrer :**

$$
\begin{aligned}
c^d \bmod N &\equiv m^{ed} \bmod N \\
&\equiv m^{1+k\phi(N)} \bmod N \quad \longleftarrow \quad ed \equiv 1 \bmod \phi(N) \Leftrightarrow \exists k \in \mathbb{Z}, ed = 1 + k \cdot \phi(N) \\
&\equiv m^1 \cdot m^{k\phi(N)} \bmod N \\
&\equiv m^1 \cdot \left(m^{\phi(N)}\right)^k \bmod N \\
&\equiv m^1 \cdot (1)^k \bmod N \quad \longleftarrow \quad \textbf{Théorème d'Euler} \\
&\equiv m^1 \bmod N
\end{aligned}
$$

R.S.A : Exemple

- **Génération des clés :**
  - On choisit $p = 7$ et $q = 11$, donc $N = 77$
  - On a $\phi(77) = \phi(7) \cdot \phi(11) = 6\times10 = 60$

R.S.A : Exemple

- **Génération des clés :**
  - On choisit $p = 7$ et $q = 11$, donc $N = 77$
  - On a $\phi(77) = \phi(7) \cdot \phi(11) = 6 \times 10 = 60$
  - On choisit $e = 13$, $pgcd(13, 60) = 1$
  - Avec Euclide étendu on calcule $d = e^{-1} = 13^{-1} \equiv 37 \bmod 60$

R.S.A : Exemple

- **Génération des clés :**
  - On choisit $p = 7$ et $q = 11$, donc $N = 77$
  - On a $\phi(77) = \phi(7) \cdot \phi(11) = 6 \times 10 = 60$
  - On choisit $e = 13$, $pgcd(13, 60) = 1$
  - Avec Euclide étendu on calcule $\mathrm{d} = \mathrm{e}^{-1} = 13^{-1} \equiv 37 \bmod 60$
  - On a $pk = (N, e) = (77{,}13)$ et $sk = (p, q, d) = (7, 11, 37)$

R.S.A : Exemple

Alice

$$101_b = 5$$

Bob

R.S.A : Exemple

Alice

$101_b = 5$

Bob

$pk = (77,13)$

$sk = (7, 11, 37)$

R.S.A : Exemple

Alice

$pk = (77,13)$

$101_b = 5$

Bob

$sk = (7, 11, 37)$

R.S.A : Exemple

Alice

$pk = (77{,}13)$

Bob

$sk = (7, 11, 37)$

$101_b = 5$ $\xrightarrow[\text{Encryption}]{}$ 26

Encryption

$5^{13} \bmod 77$

R.S.A : Exemple

Alice

$pk = (77,13)$

$101_b = 5$ → 26 → 5

Encryption

$5^{13} \bmod 77$

Bob

$sk = (7,11,37)$

Decryption

$26^{37} \bmod 77$

R.S.A

- **Génération des clés :**
  1. **Soit p et q deux grands premiers (1024 bits)**
  2. **Soit $N = p \cdot q$ (2048 bits)**
  3. **Soient e, d deux entiers premiers avec $\phi(N) = (p-1) \cdot (q-1)$ et $ed \equiv 1 \bmod \phi(N)$**
  4. **Finalement**

  Clé publique (pk) : (N, e)
  Clé secrète (sk) : (d, p, q)

- **Sécurité (Intuition) :**
  - **Pour retrouver d à partir de e il faut $\phi(N)$.**
  - **$\phi(N)$ est compliqué à calculer sans la factorisation de N**

Un peu de maths (suite & fin)

Structure de groupe

Définition :

Soit G un ensemble et $*$ une application de $G \times G$ dans G. Le couple $(G,*)$ est un groupe si et seulement si:

1. La loi $*$ est associative, $\forall (x, y, z) \in G^3, (x * y) * z = x * (y * z)$
2. Il existe $e \in G$, appelé élément neutre, $\forall x \in G, x * e = e * x = x$
3. Tout élément x de G admet un inverse noté x^{-1}, $\forall x \in G, \exists y \in G, x * y = y * x = e$

Structure de groupe

Définition :

Soit G un ensemble et $*$ une application de $G \times G$ dans G. Le couple $(G,*)$ est un groupe si et seulement si:

1. La loi $*$ est associative, $\forall (x,y,z) \in G^3, (x * y) * z = x * (y * z)$
2. Il existe $e \in G$, appelé élément neutre, $\forall x \in G, x * e = e * x = x$
3. Tout élément x de G admet un inverse noté x^{-1}, $\forall x \in G, \exists y \in G, x * y = y * x = e$

- **Ordre : l'ordre d'un élément g, noté $o(g)$ est le plus petit k tel que $g^k = e$**

Structure de groupe

Définition :

Soit G un ensemble et $*$ une application de $G \times G$ dans G. Le couple $(G, *)$ est un groupe si et seulement si:

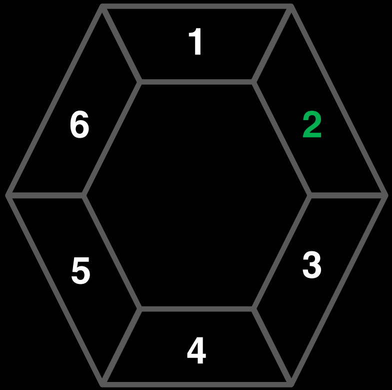
1. La loi $*$ est associative, $\forall (x, y, z) \in G^3, (x * y) * z = x * (y * z)$
2. Il existe $e \in G$, appelé élément neutre, $\forall x \in G, x * e = e * x = x$
3. Tout élément x de G admet un inverse noté x^{-1}, $\forall x \in G, \exists y \in G, x * y = y * x = e$

- **Ordre : l'ordre d'un élément g, noté $o(g)$ est le plus petit k tel que $g^k = e$**
- **Générateur : $x \in G$ est un générateur de G si tous les éléments de G peuvent s'écrire $x^k, k \in \mathbb{Z}$. On note $G = \langle x \rangle$.**

Structure de groupe

Exemple : $G = (\mathbb{Z}/7\mathbb{Z},\times) = (\{1,2,3,4,5,6\},\times)$

$x = 2$

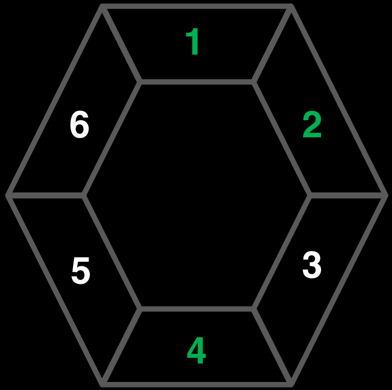


Structure de groupe

Exemple : $G = (\mathbb{Z}/7\mathbb{Z},\times) = (\{1,2,3,4,5,6\},\times)$

$x = 2$

$$x^2 \bmod 7 = 4$$
$$x^3 \bmod 7 = 1$$
$$x^4 \bmod 7 = 2$$
$$x^5 \bmod 7 = 4$$
$$x^6 \bmod 7 = 1$$



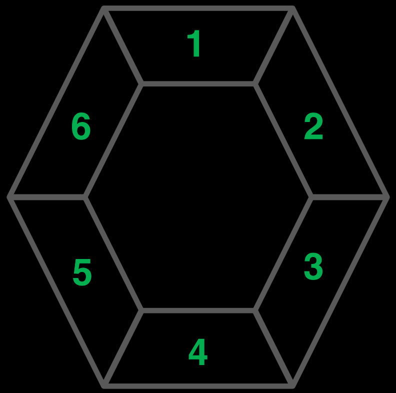
O(2) = 3, 2 n'est pas un générateur

Structure de groupe

Exemple : $G = (\mathbb{Z}/7\mathbb{Z},\times) = (\{1,2,3,4,5,6\},\times)$

$x = 3$

$$x^2 \bmod 7 = 2$$
$$x^3 \bmod 7 = 6$$
$$x^4 \bmod 7 = 4$$
$$x^5 \bmod 7 = 5$$
$$x^6 \bmod 7 = 1$$



O(3) = 6, 3 est un générateur

Le logarithme discret

Définition logarithme discret dans $\mathbb{Z}/p\mathbb{Z}$:

Soit p un nombre premier, g un élément de $(\mathbb{Z}/p\mathbb{Z})^{\times}$, r un entier et $x \equiv g^r \bmod p$.
Le problème du logarithme discret consiste à retrouver r connaissant p, g, x.

El Gamal

El Gamal

- **Génération des clés :**
  - Choisir un nombre premier p, et un générateur g de $\mathbb{Z}/p\mathbb{Z}$
  - Générer aléatoirement un entier $r \in [1, \cdots, p-1]$
  - Calculer $B \equiv g^r \bmod p$
  - On a $pk = (g, p, B)$ et $sk = r$

El Gamal

- **Génération des clés :**
  - Choisir un nombre premier p, et un générateur g de $\mathbb{Z}/p\mathbb{Z}$
  - Générer aléatoirement un entier $r \in [1, \cdots, p-1]$
  - Calculer $B \equiv g^r \bmod p$
  - On a $pk = (g, p, B)$ et $sk = r$

- **Chiffrement : message** $m \in [1, \cdots, p-1]$
  - Générer un entier aléatoire $a \in [1, \cdots, p-1]$
  - Calculer $c_1 \equiv g^a \bmod p$ et $c_2 \equiv m \cdot B^a \bmod p$
  - Message chiffré (c_1, c_2)

El Gamal

- **Génération des clés :**
  - Choisir un nombre premier p, et un générateur g de $\mathbb{Z}/p\mathbb{Z}$
  - Générer aléatoirement un entier $r \in [1, \cdots, p-1]$
  - Calculer $B \equiv g^r \bmod p$
  - On a $pk = (g, p, B)$ et $sk = r$

- **Chiffrement : message** $m \in [1, \cdots, p-1]$
  - Générer un entier aléatoire $a \in [1, \cdots, p-1]$
  - Calculer $c_1 \equiv g^a \bmod p$ et $c_2 \equiv m \cdot B^a \bmod p$
  - Message chiffré (c_1, c_2)

- **Déchiffrement :**
  - Calculer $d_1 \equiv c_1^{-1} \bmod p$ et $m \equiv c_2 \cdot d_1^r \bmod p$

El Gamal

- **Déchiffrement :**
  - Chiffré $(c_1, c_2) = (g^a \bmod p, m \cdot B^a \bmod p)$

$$\begin{aligned} c_2 \cdot (c_1^{-1})^r &= (m \cdot B^a) \cdot \left((g^a)^{-1}\right)^r \\ &= m \cdot g^{ra} \cdot (g^{-a})^r \\ &= m \cdot g^{ra-ar} \\ &= m \end{aligned}$$

El Gamal : exemple

- **Génération des clés :**
  - On prend $p = 661$ premier
  - On choisit $g = 23$ un générateur de $\mathbb{Z}/661\mathbb{Z}$
  - Générer aléatoirement un entier $r \in [1, \cdots, 660] = 7$
  - $B \equiv g^r \bmod p = 23^7 \bmod 661 = 566$
  - On a $pk = (23, 661, 566)$ et $sk = 7$

El Gamal : Exemple

Alice

$110000000_b = 192$

Bob

El Gamal : Exemple

Alice

$110000000_b = 192$

Bob

$pk = (23, 661, 566)$

$sk = 7$

El Gamal : Exemple

Alice

Bob

$pk = (23, 661, 566)$

$$110000000_b = 192 \xrightarrow[\text{Encryption}]{} (105, 237)$$

$$a = 13$$

$$c_1 = 23^{13} \bmod 661$$

$$c_2 = 192 \times 566^{13} \bmod 661$$

El Gamal : Exemple

Alice

$pk = (23, 661, 566)$

Bob

$sk = 7$

$110000000_b = 192 \longrightarrow (105, 237) \longrightarrow 192$

Encryption

$a = 13$

$c_1 = 23^{13} \bmod 661$

$c_2 = 192 \times 566^{13} \bmod 661$

Decryption

$c_2 \cdot (c_1^{-1})^7 \bmod 661$

$=$

$237 \times (105^{-1})^7 \bmod 661$

Trouver un générateur

- **Idée :**
  - Choisir un élément a aléatoirement dans $\mathbb{Z}/p\mathbb{Z}$
  - Tester $\forall i \in [2, p-2], a^i \bmod p \ \neq 1$ et $a^{p-1} \equiv 1 \bmod p$
  - Il y a $\phi(p-1)$ générateurs dans $\mathbb{Z}/p\mathbb{Z}$
  - La probabilité de tomber sur un générateur est $\frac{\phi(p-1)}{\phi(p)} = \frac{\phi(p-1)}{p-1} \in \mathcal{O}\left(\frac{1}{\log_2 \log_2 p}\right)$
    - Exemple :
      - $p = 7, \frac{\phi(7-1)}{7-1} = \frac{2}{6} \sim 0.33$
      - $p = 661, \frac{\phi(660)}{660} = \frac{160}{660} \sim 0.242$

Exponentiation rapide

- **RSA :**
  - Chiffrer : $c \equiv m^e \bmod N$
  - Déchiffrer : $m \equiv c^d \bmod N$
- **El Gamal :**
  - Chiffrer : $c_1 \equiv g^a \bmod p$ et $c_2 \equiv m \cdot B^a \bmod p$
  - Déchiffrer : $m \equiv c_2 \cdot d_1^r \bmod p$

- **Exponentiation modulaire :** $x^e \bmod m$

Exponentiation rapide

- **RSA :**
  - Chiffrer : $c \equiv m^e \bmod N$
  - Déchiffrer : $m \equiv c^d \bmod N$
- **El Gamal :**
  - Chiffrer : $c_1 \equiv g^a \bmod p$ et $c_2 \equiv m \cdot B^a \bmod p$
  - Déchiffrer : $m \equiv c_2 \cdot d_1^r \bmod p$

- **Exponentiation modulaire :** $x^e \bmod m$

Input : $x \in \mathbb{Z}$, $e \in \mathbb{N}$, $n \in \mathbb{N}$, $n \geq 2$
Output : $x^e \bmod n$

$r \longleftarrow 1$
$b \longleftarrow b \bmod n$
While $e > 0$**:**
  If $e \bmod 2 == 1$**:**
    $r \longleftarrow r \cdot b \bmod n$
  $b \longleftarrow b^2 \bmod n$
  $e \longleftarrow \left\lfloor \frac{e}{2} \right\rfloor$
Return r

Exponentiation rapide

- **RSA :**
  - Chiffrer : $c \equiv m^e \bmod N$
  - Déchiffrer : $m \equiv c^d \bmod N$
- **El Gamal :**
  - Chiffrer : $c_1 \equiv g^a \bmod p$ et $c_2 \equiv m \cdot B^a \bmod p$
  - Déchiffrer : $m \equiv c_2 \cdot d_1^r \bmod p$

- **Exponentiation modulaire :** $x^e \bmod m$

Input : $x \in \mathbb{Z}$, $e \in \mathbb{N}$, $n \in \mathbb{N}$, $n \geq 2$
Output : $x^e \bmod n$

$r \longleftarrow 1$
$b \longleftarrow b \bmod n$
While $e > 0$:
  If $e \bmod 2 == 1$:
    $r \longleftarrow r \cdot b \bmod n$
  $b \longleftarrow b^2 \bmod n$
  $e \longleftarrow \left\lfloor \frac{e}{2} \right\rfloor$
Return r

Cause un problème de sécurité. **Pourquoi ?**

Exponentiation rapide

- **RSA :**
  - Chiffrer : $c \equiv m^e \bmod N$
  - Déchiffrer : $m \equiv c^d \bmod N$
- **El Gamal :**
  - Chiffrer : $c_1 \equiv g^a \bmod p$ et $c_2 \equiv m \cdot B^a \bmod p$
  - Déchiffrer : $m \equiv c_2 \cdot d_1^r \bmod p$

- **Exponentiation modulaire : $x^e \bmod m$**

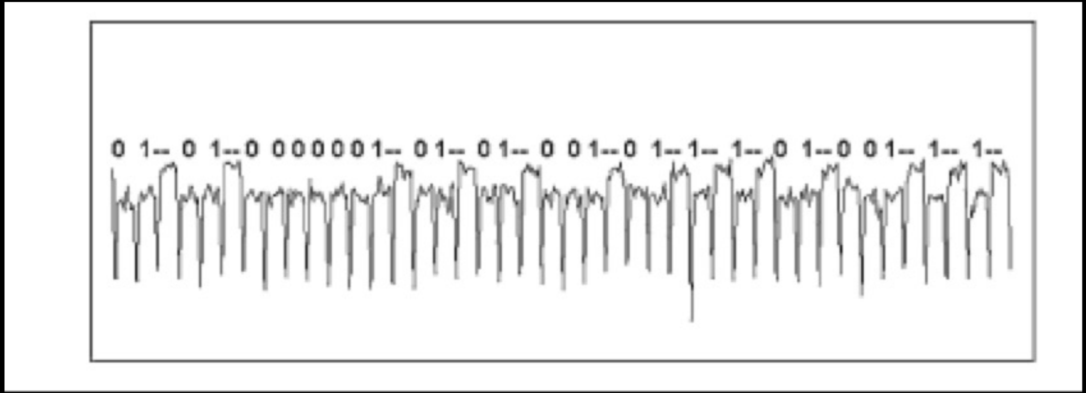
Input : $x \in \mathbb{Z}$, $e \in \mathbb{N}$, $n \in \mathbb{N}$, $n \geq 2$
Output : $x^e \bmod n$

$r \longleftarrow 1$
$b \longleftarrow b \bmod n$
While $e > 0$:
    If $e \bmod 2 == 1$:
        $r \longleftarrow r \cdot b \bmod n$
    $b \longleftarrow b^2 \bmod n$
    $e \longleftarrow \left\lfloor \frac{e}{2} \right\rfloor$
Return r

Cause un problème de sécurité. Pourquoi ?
Le nombre de multiplications dépends de la décomposition binaire de l'exposant.

Attaques par canaux cachés

- **Un attaquant retrouve la clé secrète en observant la machine**
  - Attaques temporelles
  - Attaques par analyse de consommation électrique
  - Attaques par analyse sonore
  - Attaques par le champs électromagnétique
  - …



Exponentiation rapide

- **Exponentiation modulaire :** $x^e \bmod m$

Input : $x \in \mathbb{Z}$, $e \in \mathbb{N}$, $n \in \mathbb{N}$, $n \geq 2$
Output : $x^e \bmod n$

$r \leftarrow 1$
$b \leftarrow b \bmod n$
While $e > 0$:
  If $e \bmod 2 == 1$:
    $r \leftarrow r \cdot b \bmod n$
  $b \leftarrow b^2 \bmod n$
  $e \leftarrow \left\lfloor \frac{e}{2} \right\rfloor$
Return r

Input : $x \in \mathbb{Z}$, $e \in \mathbb{N}$, $n \in \mathbb{N}$, $n \geq 2$
Output : $x^e \bmod n$

$r \leftarrow 1$
$b \leftarrow b \bmod n$
While $e > 0$:
  $\alpha \leftarrow e \bmod 2$
  $r \leftarrow r \cdot b^\alpha \bmod n$
  $b \leftarrow b^2 \bmod n$
  $e \leftarrow \left\lfloor \frac{e}{2} \right\rfloor$
Return r

Exponentiation rapide

- **Même si la théorie prouve la sécurité, il faut faire attention à la mise en pratique**

- **Il y a en tread-off à trouver entre rapidité et sécurité**

- **L’implémentation de protocole cryptographique pour la production demande beaucoup d’expérience**
  - Audits de code
  - On utilise les librairies spécialisées et auditées (openssl, …)

Cryptographie asymétrique

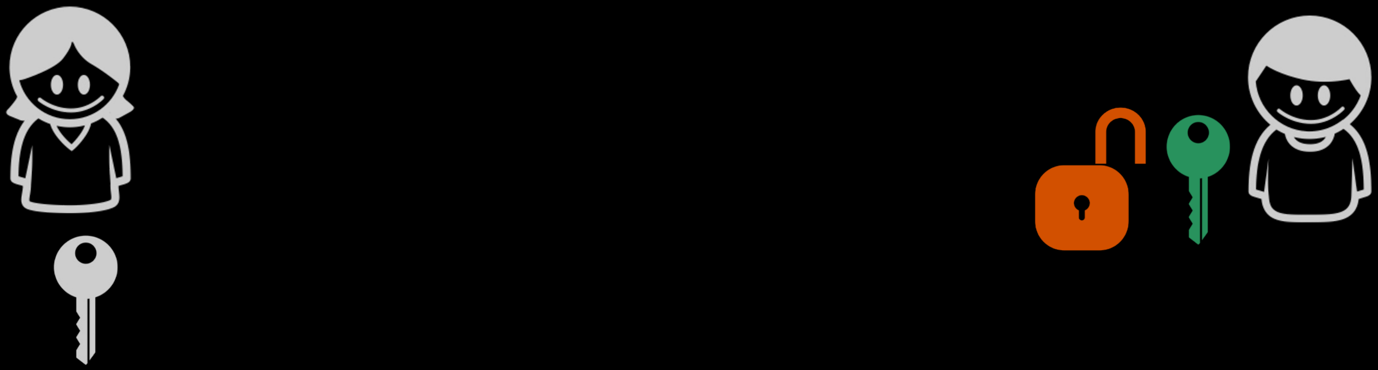
- **Permet de pouvoir s'échanger des messages sans avoir une clé en commun**

- **Bien plus coûteux que la cryptographie symétrique**
  - Dans la pratique on commine les deux approches :
    - Alice et Bob s'échangent la clé symétrique de façon sécurisé avec la cryptographie asymétrique

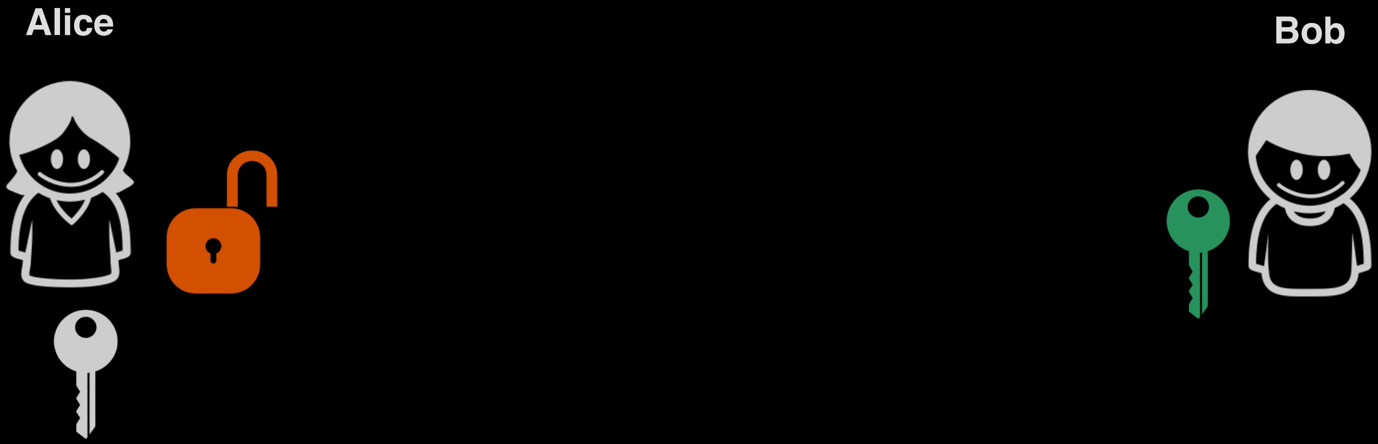
Communication sécurisée

Alice

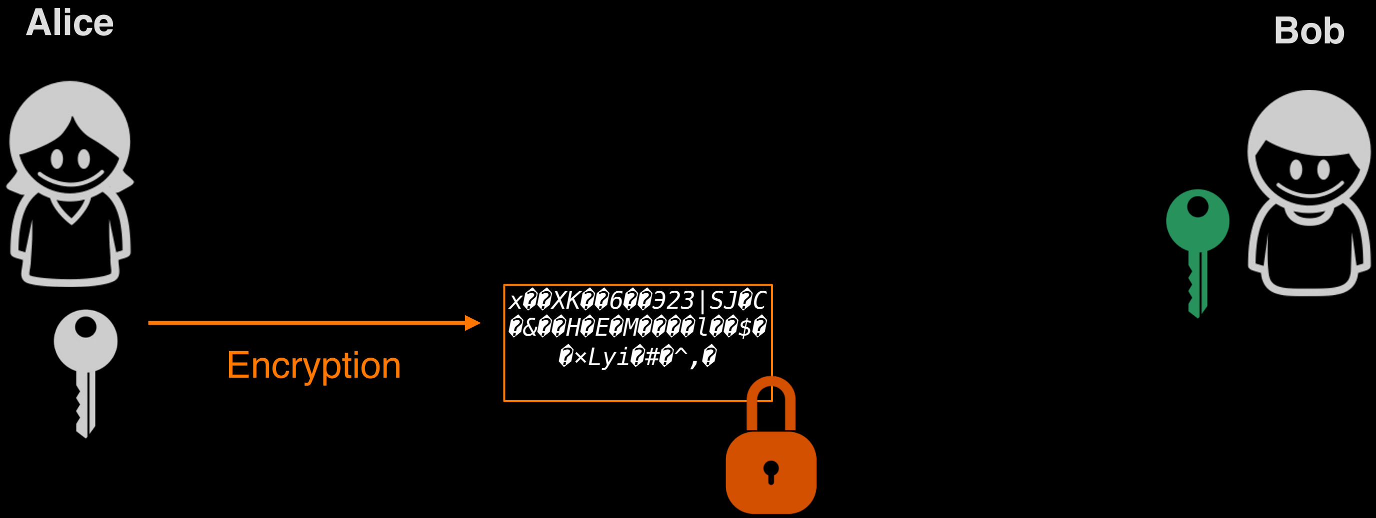
Bob



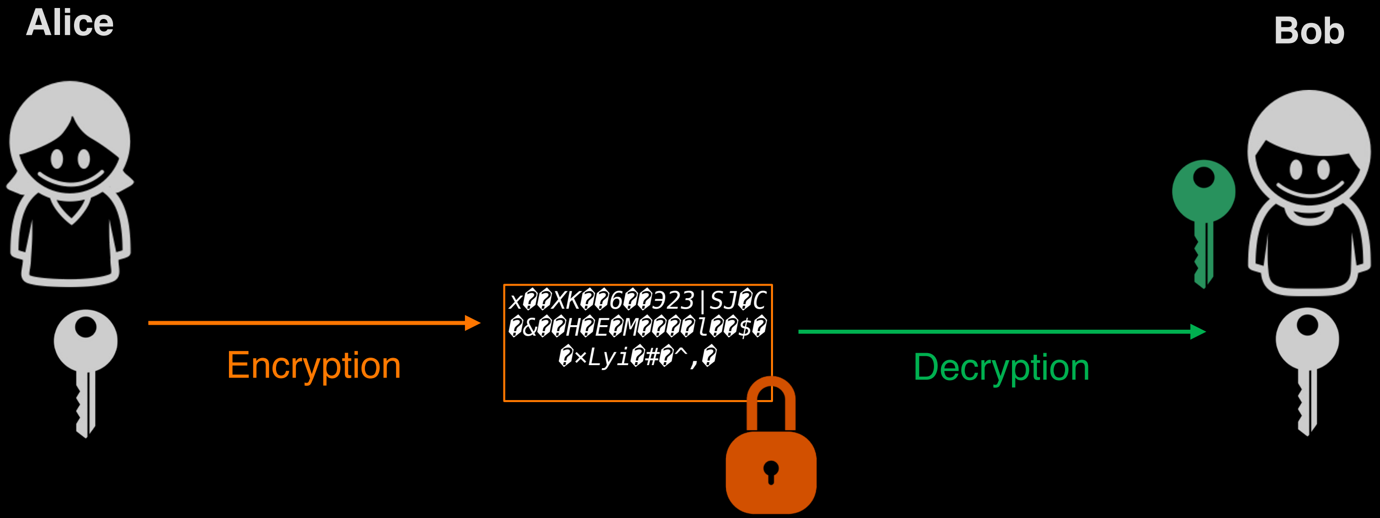
Communication sécurisée



Communication sécurisée



Communication sécurisée



Communication sécurisée