Cryptographie

Răzvan Bărbulescu

20 juillet 2013, Montpellier

Invention de la cryptographie il y a 2000 ans

César

soldat

Bonus

Invention de la cryptographie il y a 2000 ans

César

soldat

Bonus

salutare$\mapsto$tbkvubsf

Invention de la cryptographie il y a 2000 ans

César

soldat

Bonus

salutare$\mapsto$tbkvubsf

tbkvubsf$\mapsto$salutare

Crypto symétrique

- Les deux personnes qui veulent communiquer de manière confidentielle se sont déjà rencontrés pour échanger une clé secrète, un code ou un secret.
- On peut faire des translations, permutations ou autres.
- Elle est utilisés aujourd'hui sur internet.

Translation

On translate l'alphabet, par exemple d'une position vers la gauche.

	a	b	c	d	e	f	$\cdots$	q	r	s	t	u	v	w	x	y	z
a	b	c	d	e	f	$\cdots$	q	r	s	t	u	v	w	x	y	z	

a$\mapsto$b ; b$\mapsto$c ; salutare$\mapsto$tbkvubsf

Attention ! seulement 26 possibilités à essayer.

Permutations

- On choisit une permutation quelconque des 26 lettres de l'alphabet $\Rightarrow 26! = 4,03 \cdot 10^{26}$ possibilités. Enigma était un amélioration de cette idée.
- La NIST et l'ANSSI recommandent $2^{128} = 3.40 \cdot 10^{38}$ clés possibles afin d'avoir une bonne sécurité.
- Loi de Moore : La puissance de calcule des ordinateurs double tous les 18 mois.

Permutations

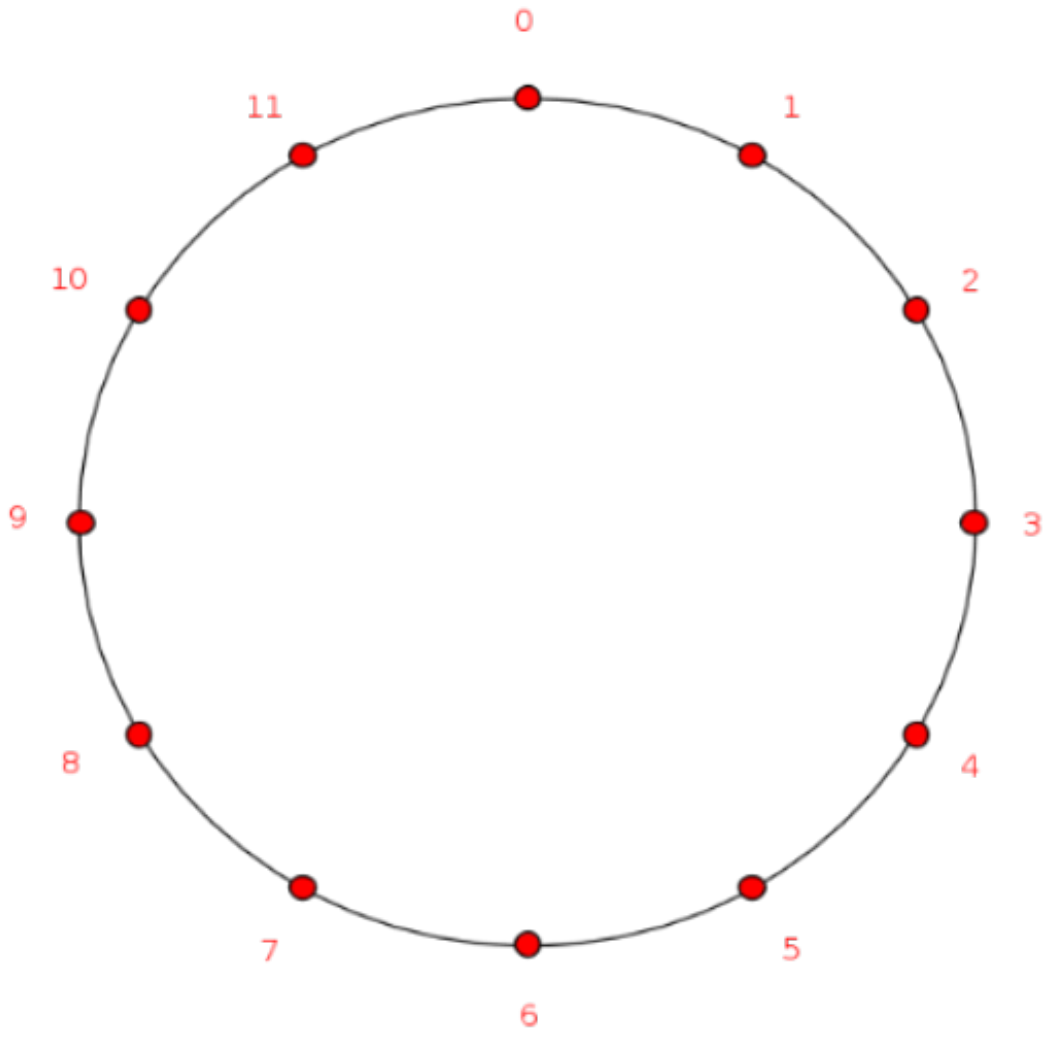
- On choisit une permutation quelconque des 26 lettres de l'alphabet $\Rightarrow 26! = 4,03 \cdot 10^{26}$ possibilités. Enigma était un amélioration de cette idée.
- La NIST et l'ANSSI recommandent $2^{128} = 3.40 \cdot 10^{38}$ clés possibles afin d'avoir une bonne sécurité.
- Loi de Moore : La puissance de calcule des ordinateurs double tous les 18 mois.
- On travaille bloc par bloc. Par exemple le verlan. Alphabet aussi grand qu'on veut.

Cryptographie asymétrique

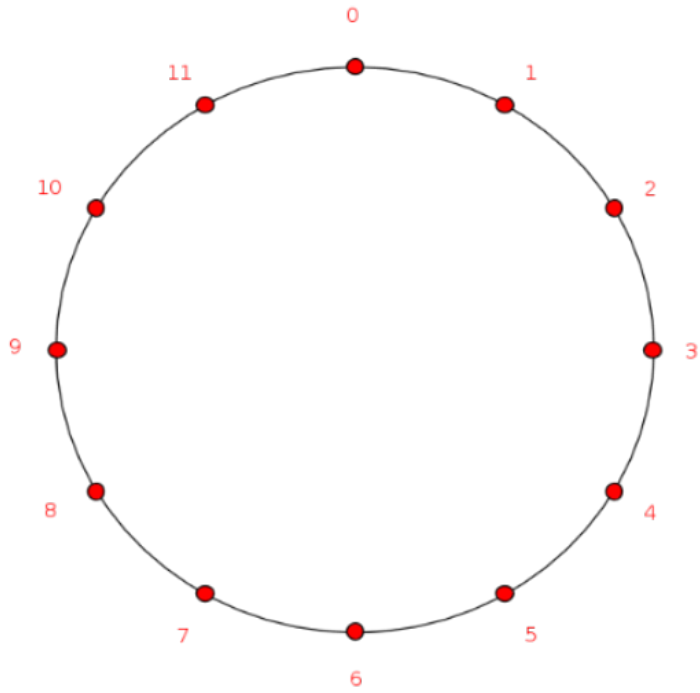
- Les deux personnes ne se sont jamais vues.
- Inventée en 1976.
- Exemple : la boite à cadenas.

Cryptographie asymétrique

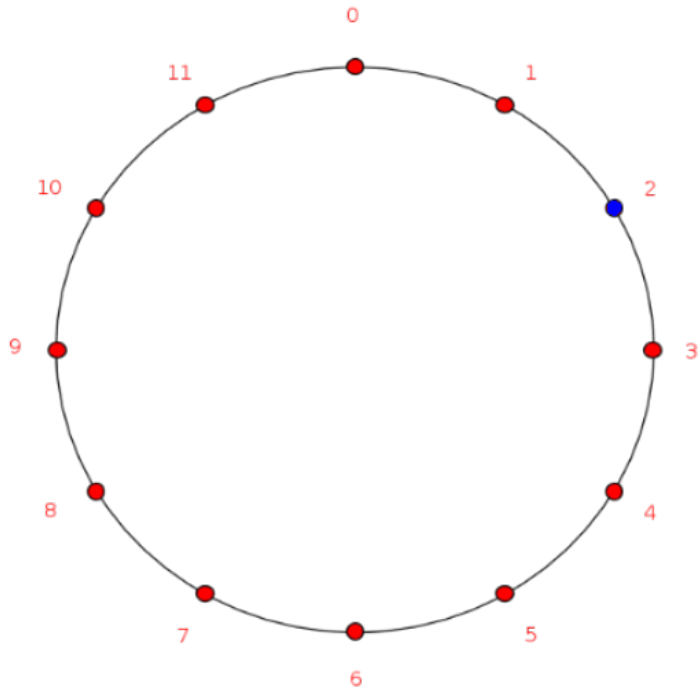
- Les deux personnes ne se sont jamais vues.
- Inventée en 1976.
- Exemple : la boite à cadenas.
- Il vaut mieux commencer par échanger une clé privée. Ensuite on fait de la crypto symétrique.


0
1
2
3
4
5
6
7
8
9
10
11

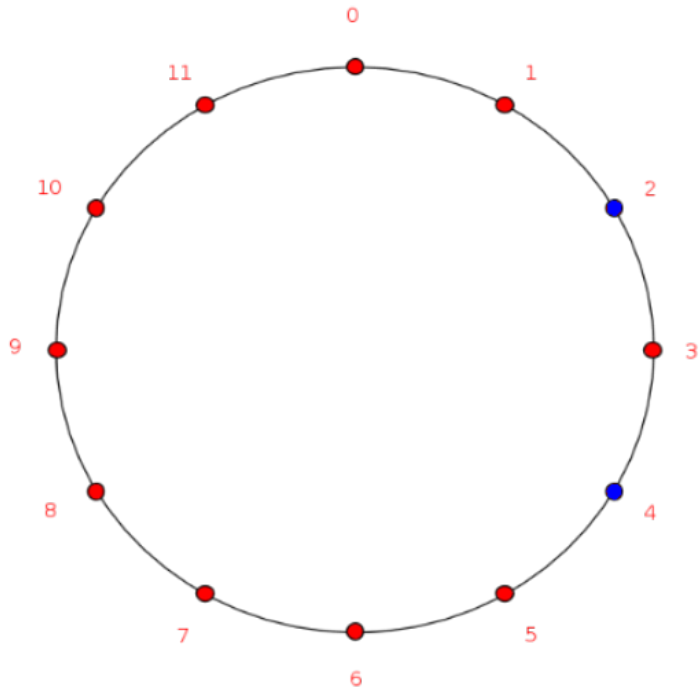
Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



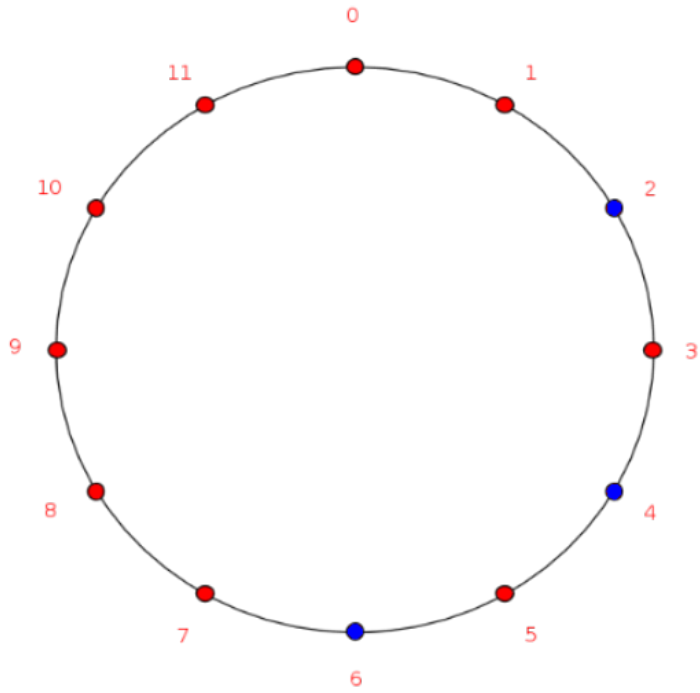
Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



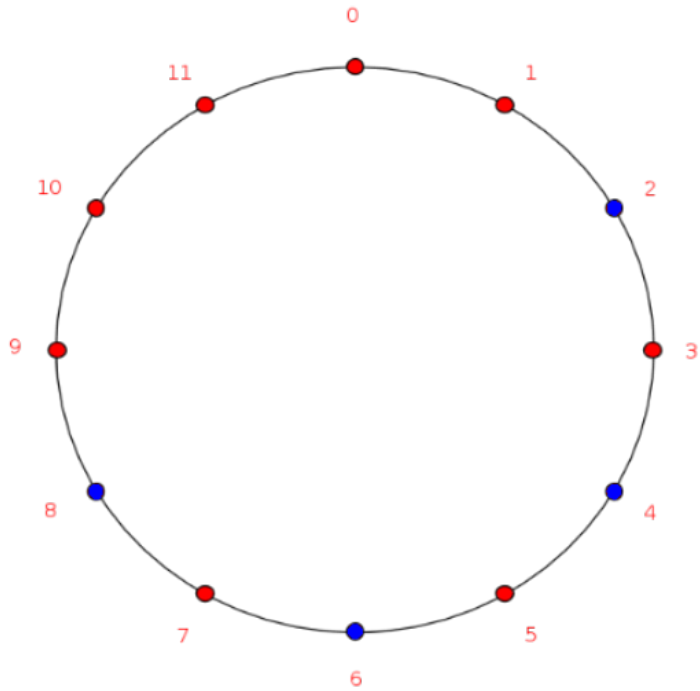
Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



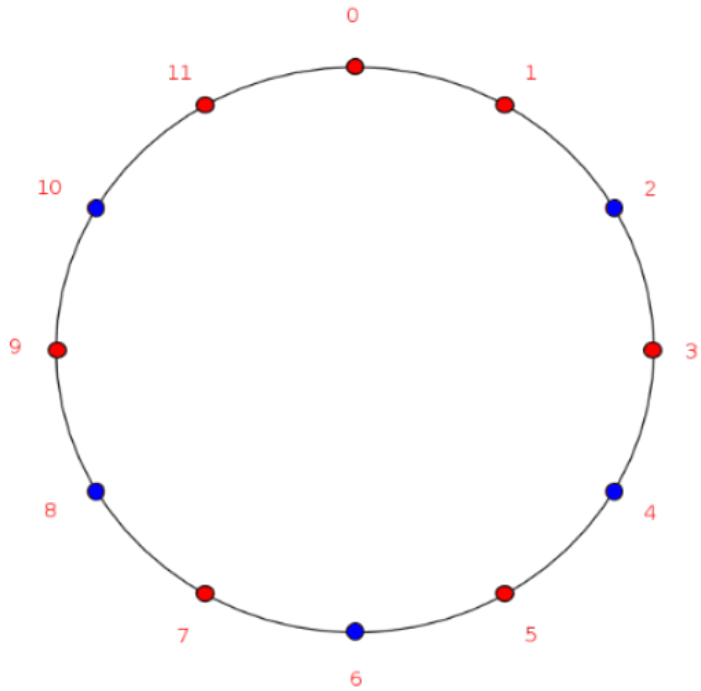
Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



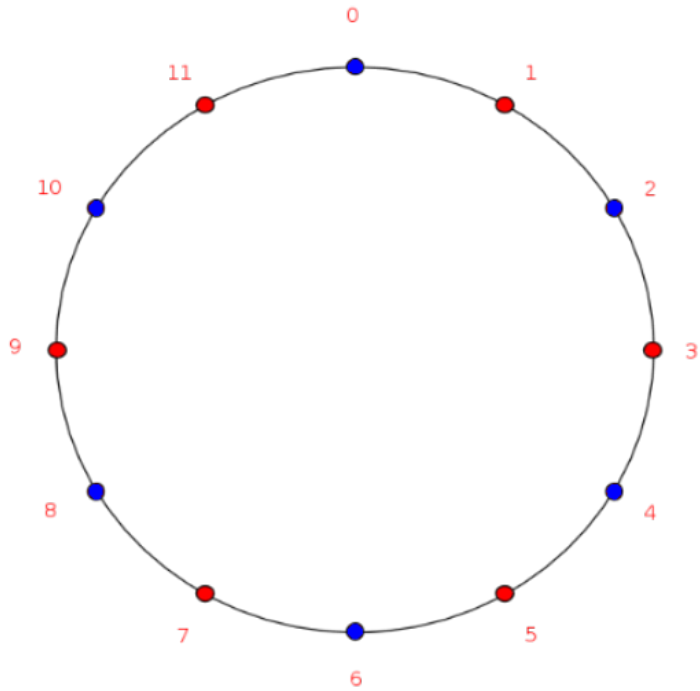
Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



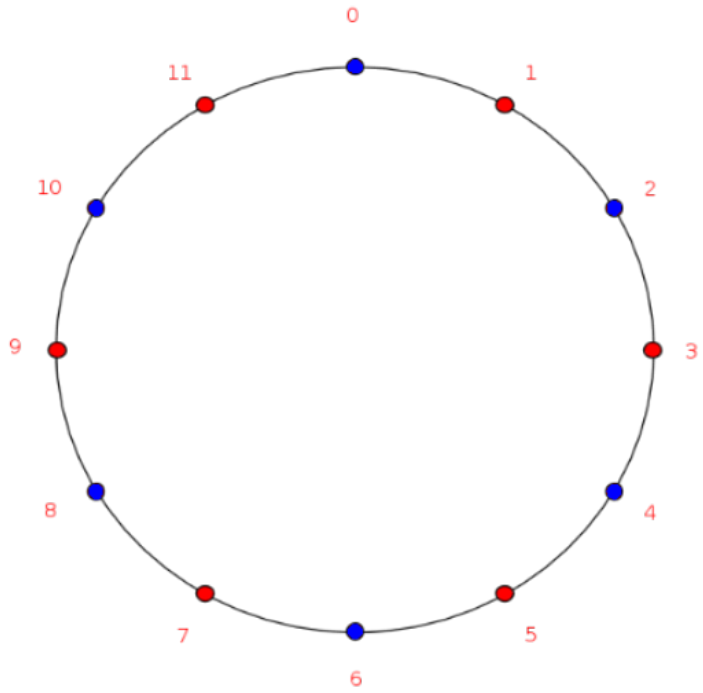
Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$

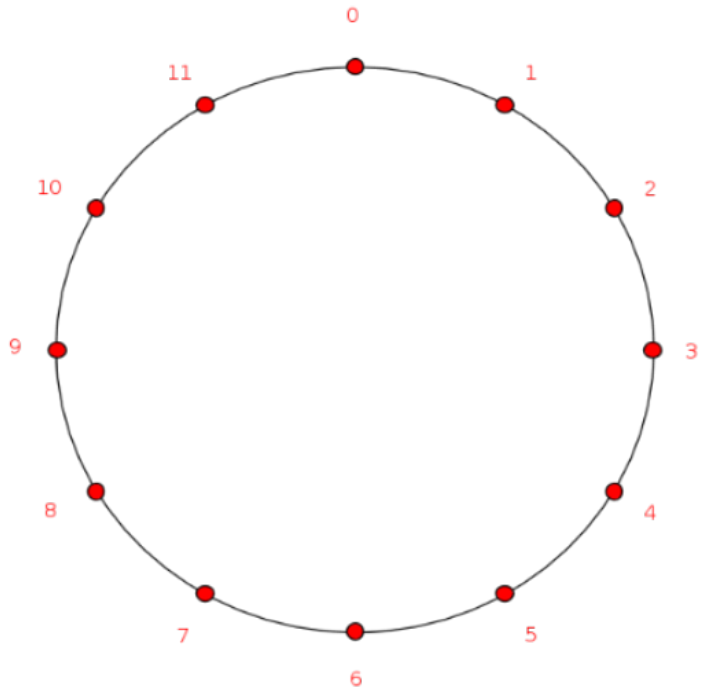


Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



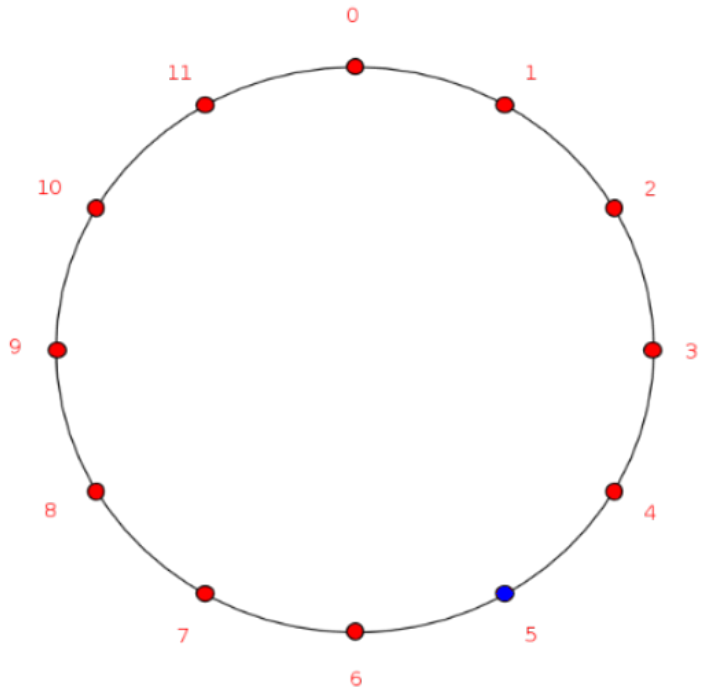
ord(2)=6

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



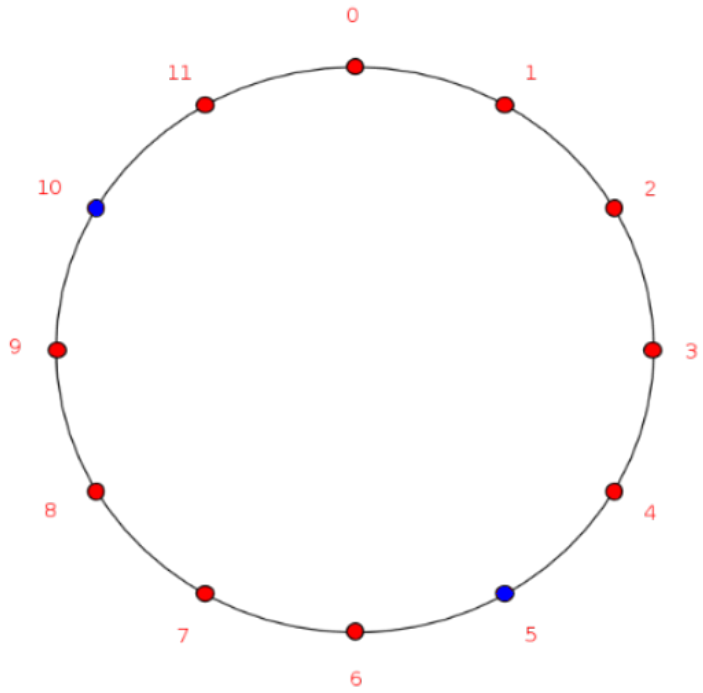
$$\mathrm{ord}(a) = \frac{12}{\mathrm{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



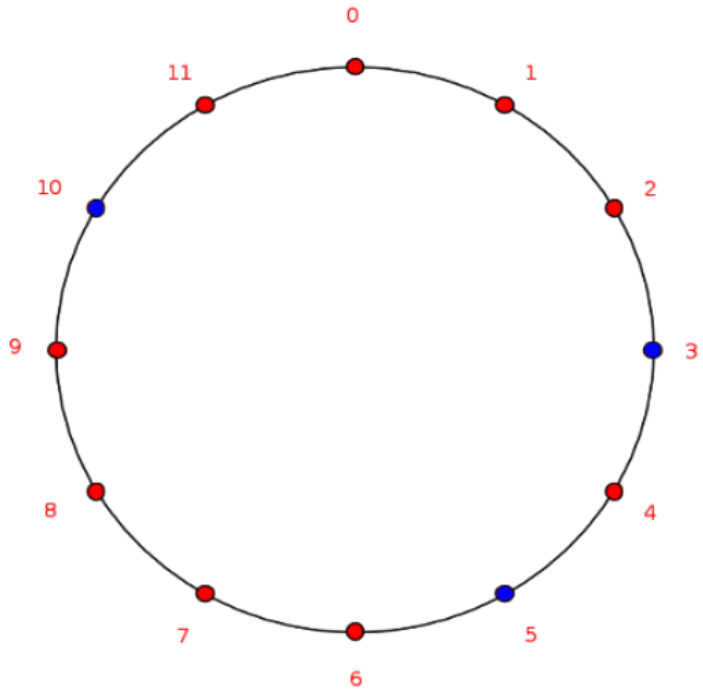
$$\mathrm{ord}(a) = \frac{12}{\mathrm{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



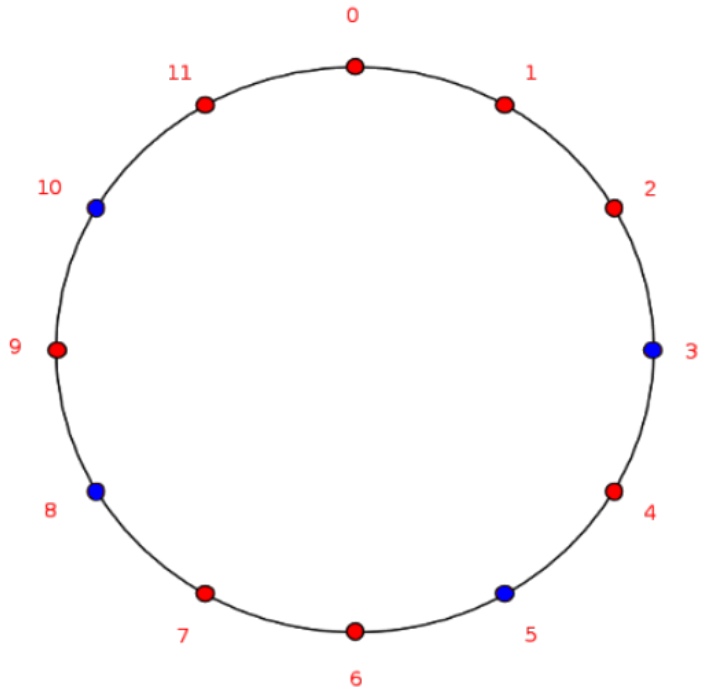
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



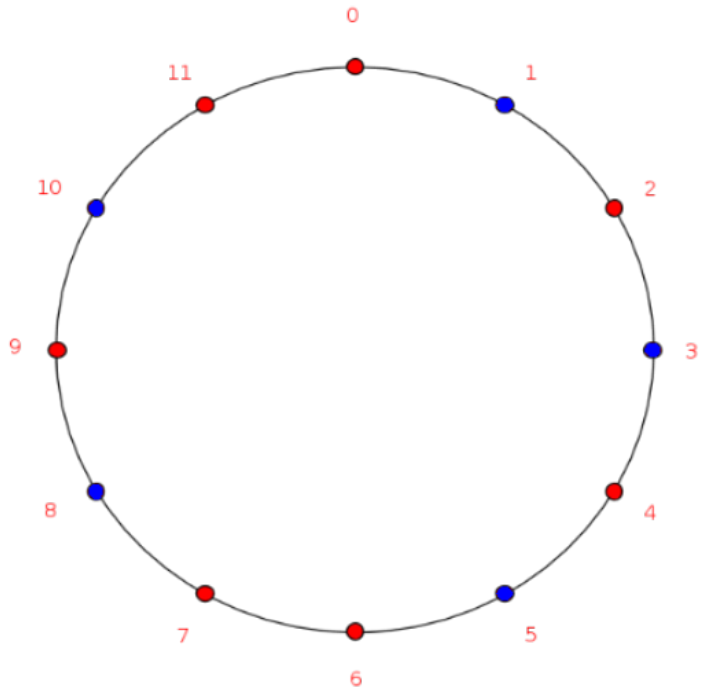
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



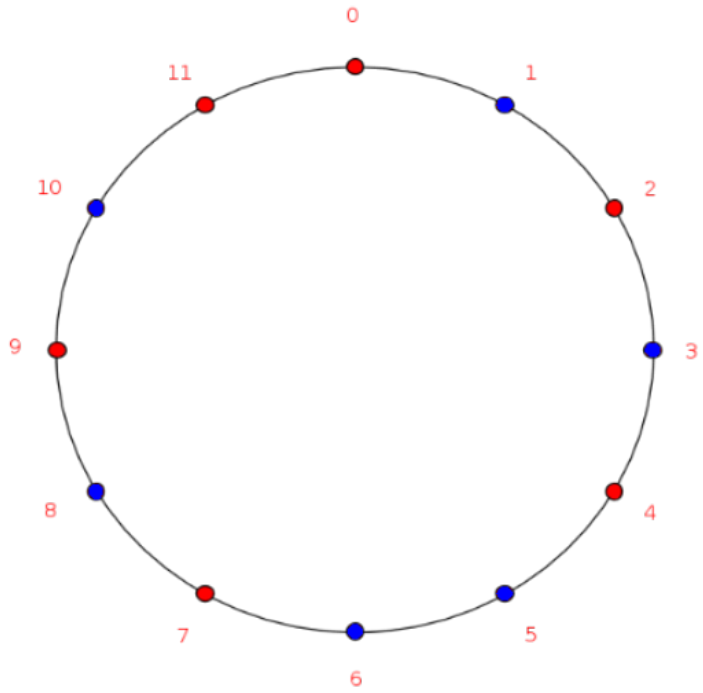
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



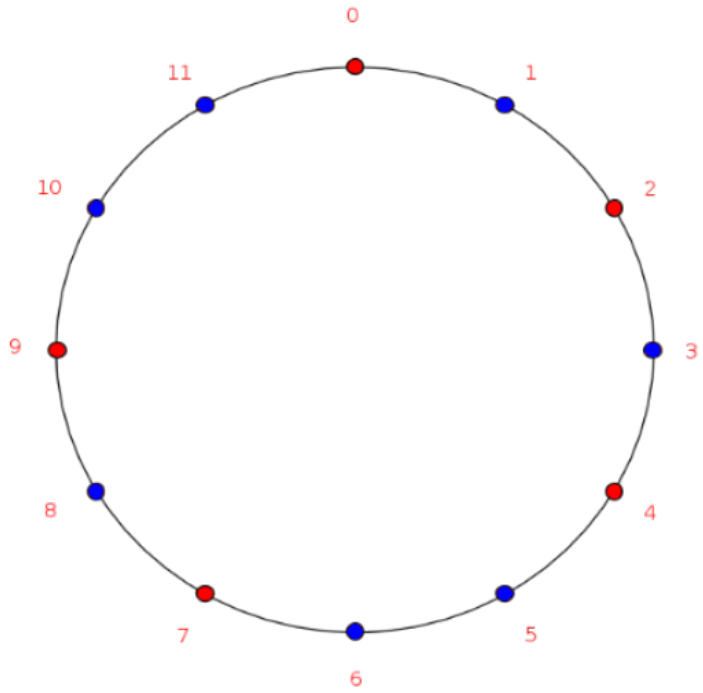
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



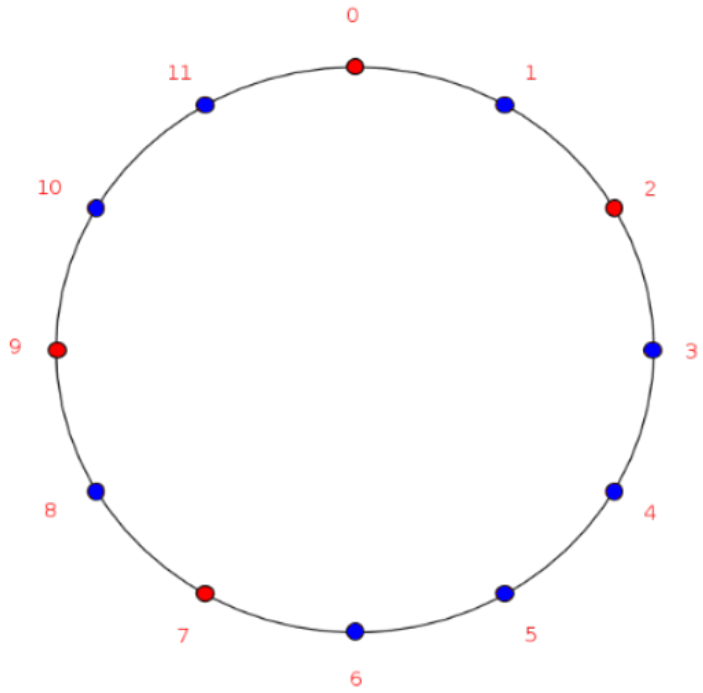
$$\mathrm{ord}(a) = \frac{12}{\mathrm{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



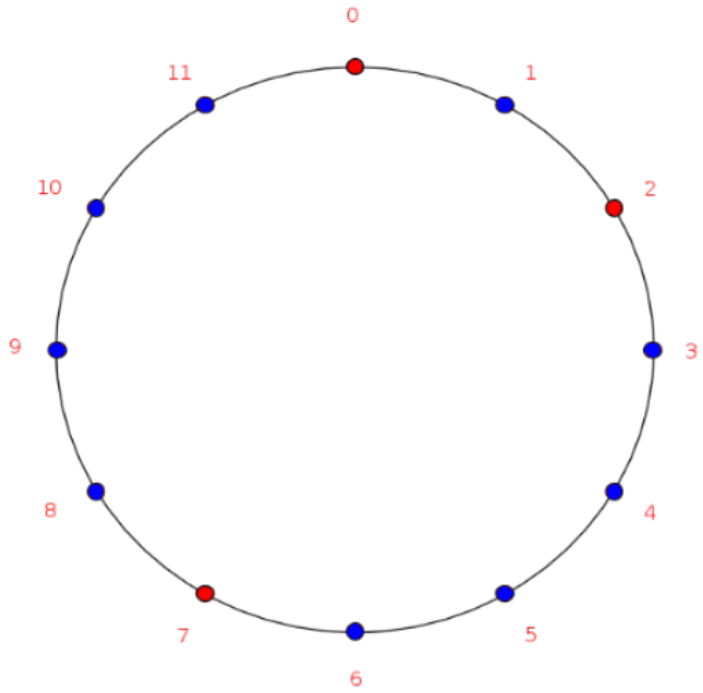
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



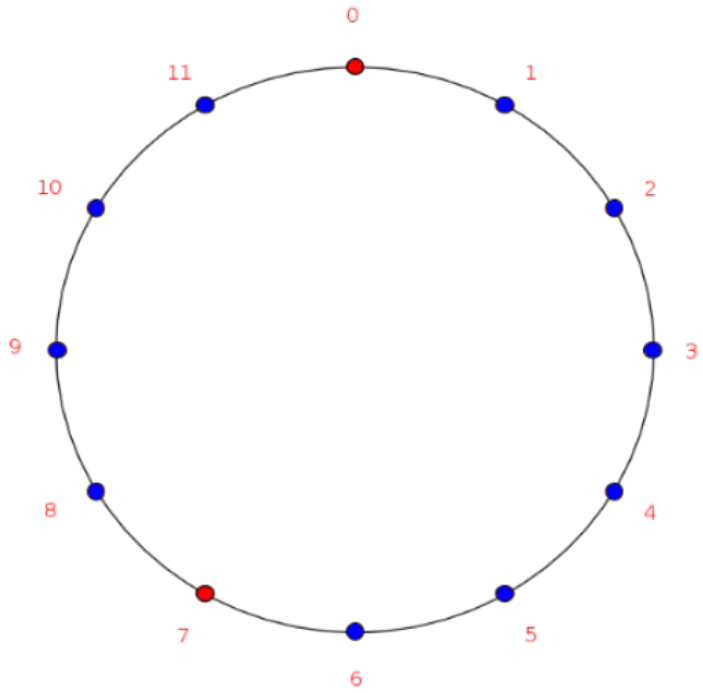
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



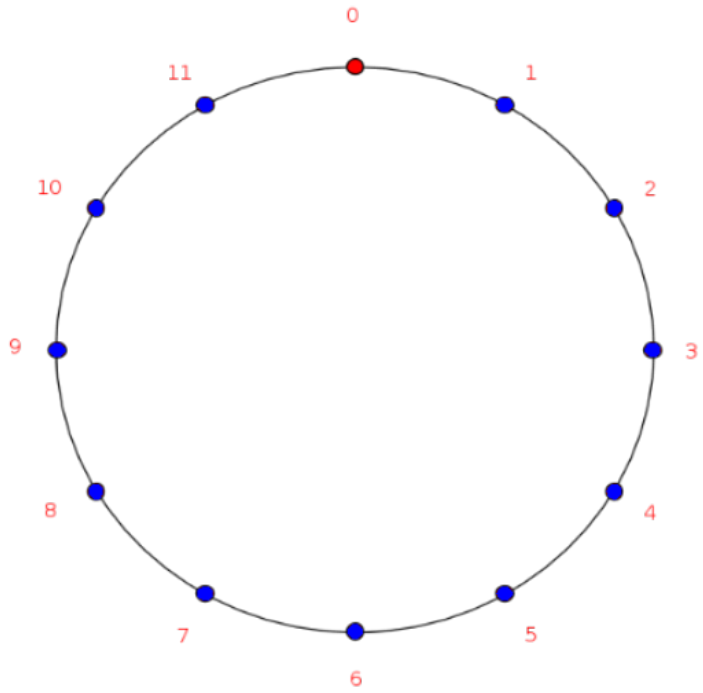
$$\mathrm{ord}(a) = \frac{12}{\mathrm{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



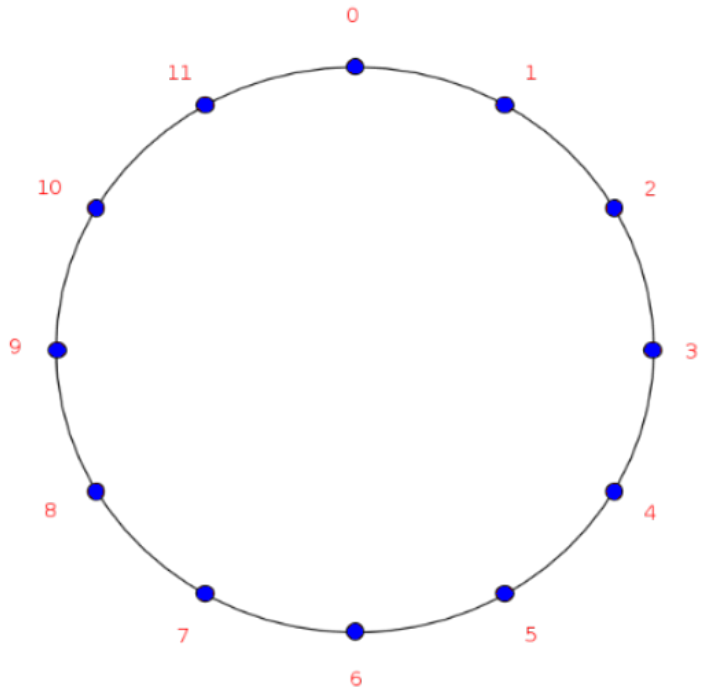
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



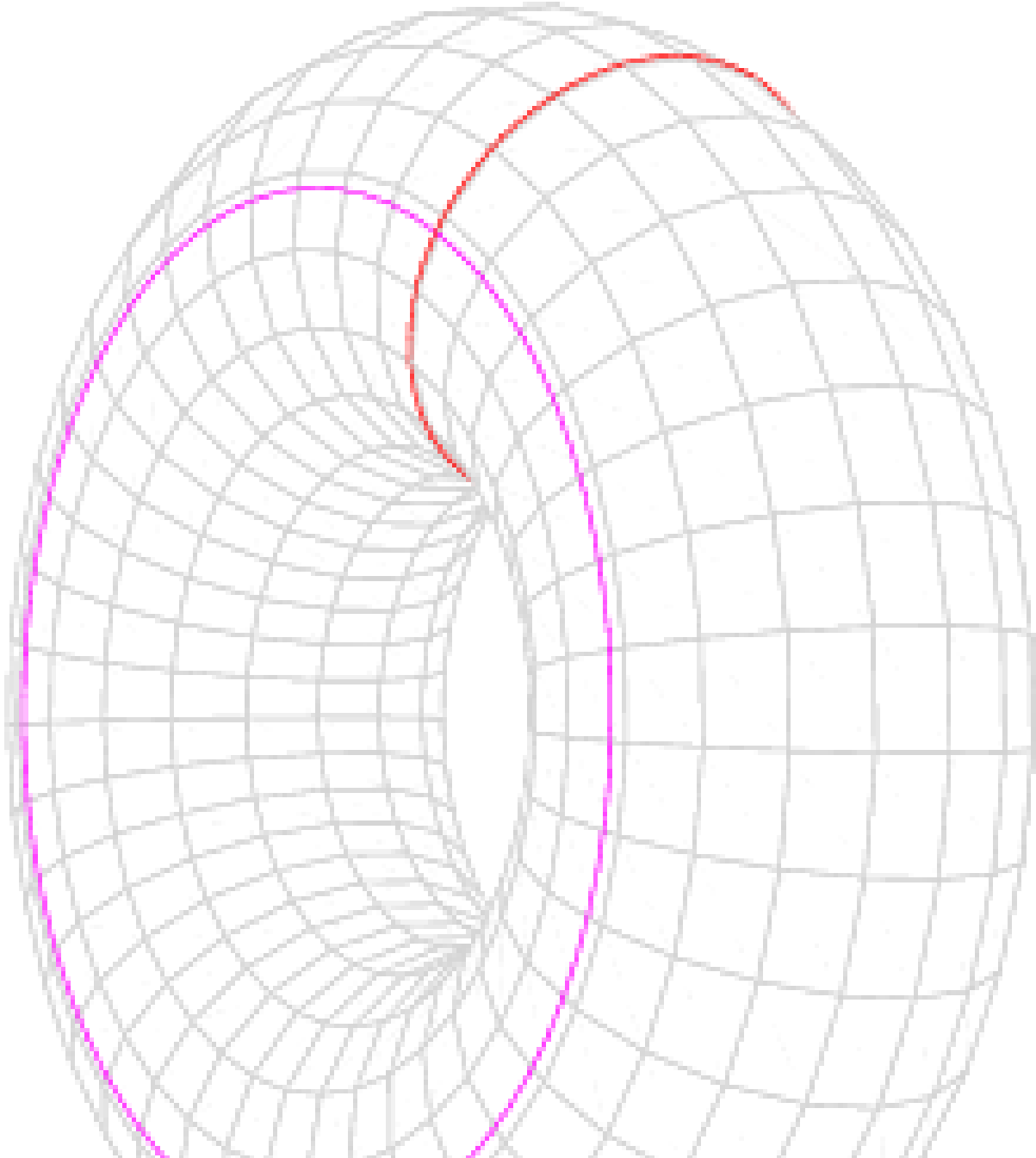
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

Le groupe $(\mathbb{Z}/12\mathbb{Z}, +)$



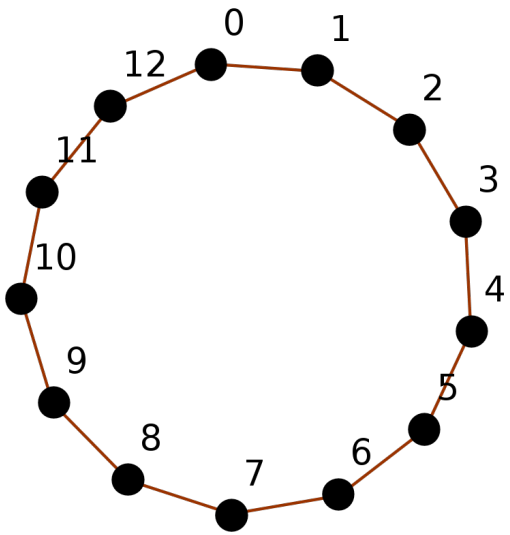
$$\text{ord}(a) = \frac{12}{\text{pgcd}(a, 12)}$$

C'est quoi un anneau ?

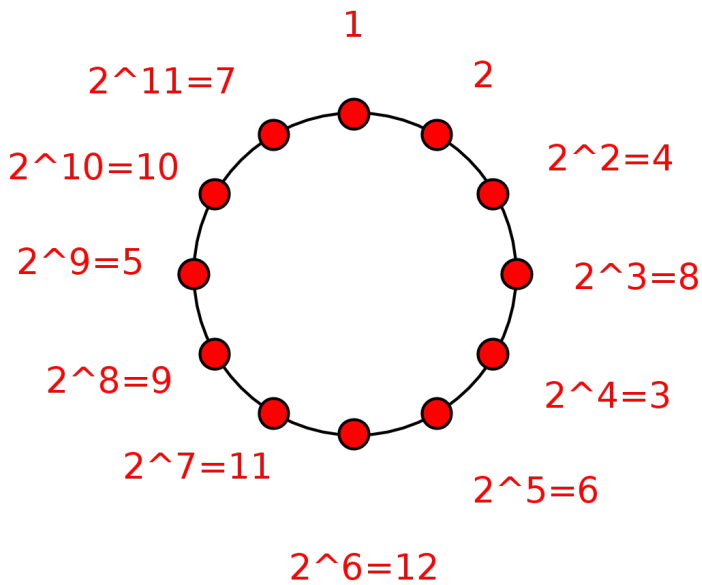


L'anneau $(\mathbb{Z}/13\mathbb{Z}, +, *)$

$(\mathbb{Z}/13\mathbb{Z}, +)$



$((\mathbb{Z}/13\mathbb{Z})^*, \times)$



Quelques questions ? $n^\circ 1$

Peut-on remplacer 2 par 3 ? c'est-à-dire, a-t-on
$\{1, 2, \ldots, 12\} = \{1, 3 \bmod 13, 3^2 \bmod 13, \ldots, 3^{12} \bmod 13\}$?

Quelques questions ? $n^\circ 1$

Peut-on remplacer 2 par 3 ? c'est-à-dire, a-t-on $\{1, 2, \ldots, 12\} = \{1, 3 \bmod 13, 3^2 \bmod 13, \ldots, 3^{12} \bmod 13\}$?
Réponse : Non car $3^3 = 27 \equiv 1 \bmod 13$. Par contre 6 marche ; il suffit de vérifier que l'ordre de 6 n'est pas un diviseur de $\#(\mathbb{Z}/13\mathbb{Z})^* = 12$. On a $6^4 \equiv 9 \bmod 13$ et $6^6 \equiv 12 \bmod 13$.

Quelques questions ? $n^\circ 2$

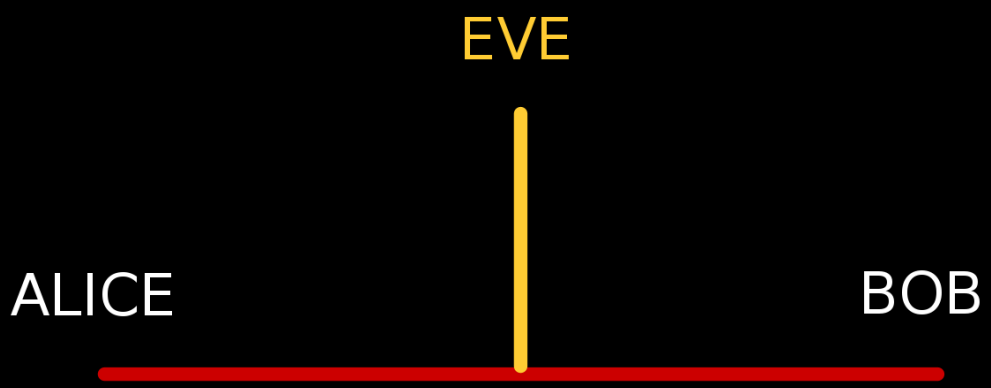
Y-a-t-il des familles connues de premiers où 3 est toujours générateur ?

Quelques questions ? $n^\circ 2$

Y-a-t-il des familles connues de premiers où 3 est toujours générateur ?
Réponse : Oui, les premiers de Fermat. Ce sont les nombres $F_n := 2^{2^n} + 1$ qui sont premiers. En effet, il suffit de vérifier que $3^{(F_n-1)/2} \equiv -1 \bmod F_n$. Pour cela on utilise la Loi de réciprocité quadratique.

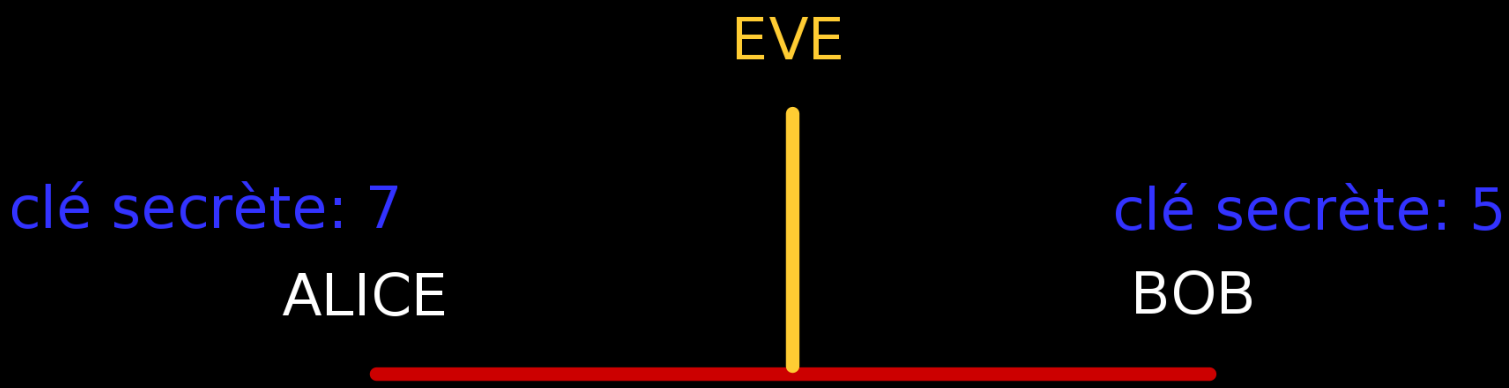
Echange de clé à la Diffie-Hellman

$$((\mathbb{Z}/13\mathbb{Z})^*, \times), \text{ generator} : 2$$



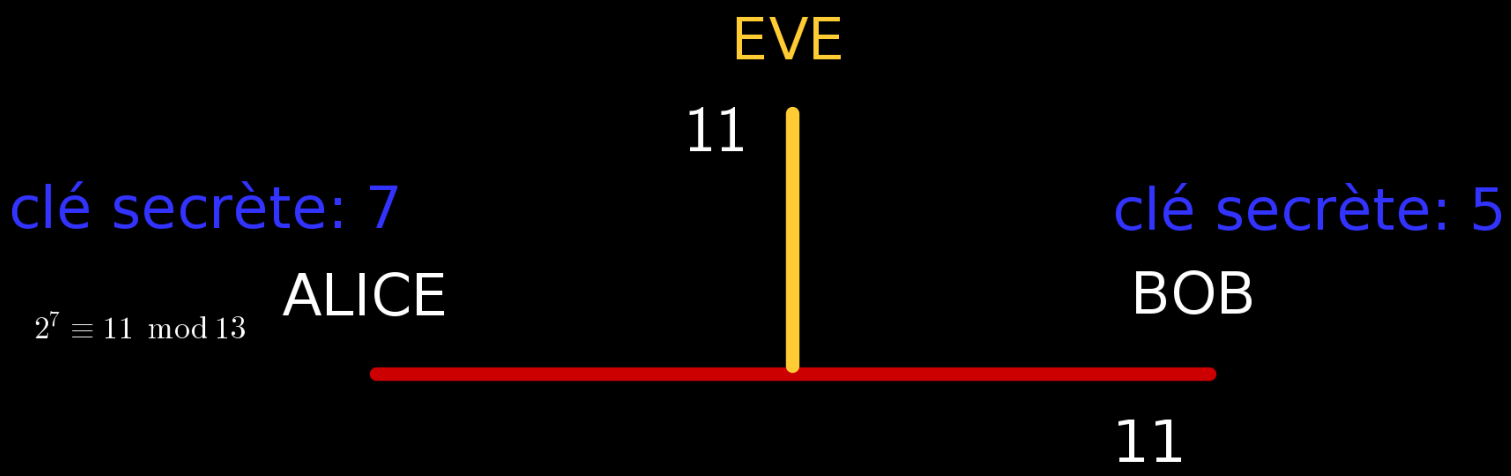
Echange de clé à la Diffie-Hellman

$$((\mathbb{Z}/13\mathbb{Z})^*, \times), \text{ generator} : 2$$



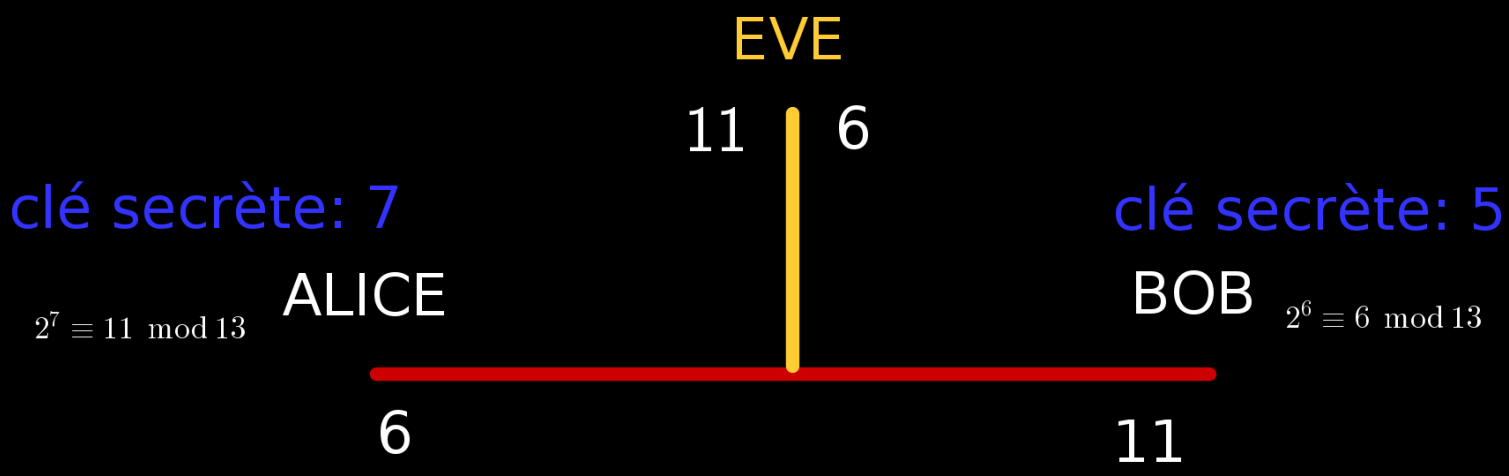
Echange de clé à la Diffie-Hellman

$$((\mathbb{Z}/13\mathbb{Z})^*, \times), \text{ generator} : 2$$



Echange de clé à la Diffie-Hellman

$$((\mathbb{Z}/13\mathbb{Z})^*, \times), \text{ generator} : 2$$



Echange de clé à la Diffie-Hellman

$$((\mathbb{Z}/13\mathbb{Z})^*, \times), \text{ generator} : 2$$

Pourquoi ça marche ?

Pourquoi ça marche ?

Alice et Bob ont calculé la même chose de de façons différentes :

$$\begin{aligned} 6^7 \equiv (2^5)^7 &\equiv 2^{35} \\ 11^5 \equiv (2^7)^5 &\equiv 2^{35}. \end{aligned}$$

Pourquoi Eve ne pe pas trouver 7 ?

$$((\mathbb{Z}/13\mathbb{Z})^*, \times), \text{ generator} : 2$$

Mettons nous à la place d'Eve

La science qui analyse la sécurité d'un cryptosystème s'appelle *cryptanalyse*. cryptologie=cryptanalyse+cryptographie.

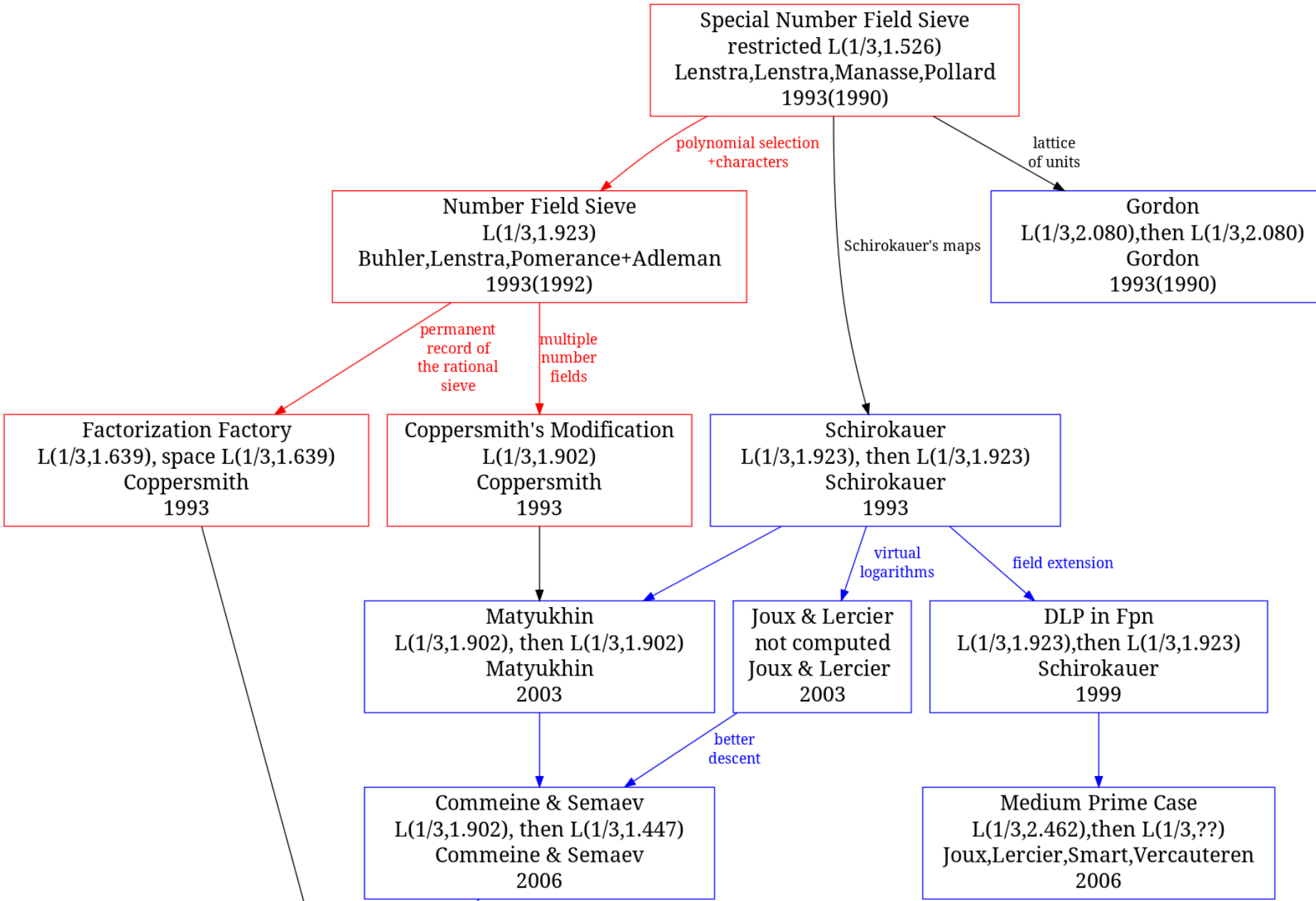
Mettons nous à la place d'Eve

La science qui analyse la sécurité d'un cryptosystème s'appelle *cryptanalyse*. cryptologie=cryptanalyse+cryptographie.

Soit p un nombre premier, g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ et h un autre élément de $(\mathbb{Z}/p\mathbb{Z})^*$. Le problème du logarithm discret consiste à trouver le plus petit nombre naturel x tel que

$$g^x = h.$$

Un peu d'histoire



Le futur

Le futur

- *à court terme :* On va remplacer le logarithme discret dans les corps finis par le problème équivalent sur les courbes elliptiques. Celles-ci sont définies pour chaque couple a et b comme l'ensemble des solutions (x, y) de l'équiation $y^2 = x^3 + ax + b$.

Le futur

- *à court terme :* On va remplacer le logarithme discret dans les corps finis par le problème équivalent sur les courbes elliptiques. Celles-ci sont définies pour chaque couple a et b comme l'ensemble des solutions (x, y) de l'équiation $y^2 = x^3 + ax + b$.

- *à long terme :* On cherchera une fonction à sens unique pour laquelle on pourra faire des preuves.

Le futur

- *à court terme :* On va remplacer le logarithme discret dans les corps finis par le problème équivalent sur les courbes elliptiques. Celles-ci sont définies pour chaque couple a et b comme l'ensemble des solutions (x, y) de l'équiation $y^2 = x^3 + ax + b$.

- *à long terme :* On cherchera une fonction à sens unique pour laquelle on pourra faire des preuves.

- *à très long terme :* On pourra également appliquer les outils développés par les cryptologues dans d'autres domaines comme la chimie ou la robotique.

Merci. Questions ?