Mathématiques discrètes

Michel Rigo

http://www.discmath.ulg.ac.be/

Année 2007–2008

Plan du cours

- "Algèbre" → corps (champs) finis
  - Construction, propriétés,...
  - Applications : codes correcteurs, ...
- Cryptographie
  - Cryptographie "classique" à clé secrète
  - Cryptographie à clé publique, RSA
  - RSA et sa mise en oeuvre (nombres premiers,...)
  - Logarithme discret, ElGamal,...
- Suites linéaires récurrentes (sur un anneau quelconque)
  - Premières propriétés
  - Cas d'un champ fini
  - Séries formelles et fonctions génératrices
  - Problèmes de dénombrement (nombres de Catalan)

Rappels - mise à niveau en algèbre

Définition : groupe $(G, \circ)$ ou $(G, \circ, e)$

Un groupe : ensemble G
opération interne et partout définie $\circ : G \times G \to G$ t.q.

- $\circ$ est associative : $\forall x, y, z \in G,\ x \circ (y \circ z) = (x \circ y) \circ z$
- élément (unique) $e \in G$ neutre t.q.

$$x \circ e = x = e \circ x,\ \forall x \in G,$$

- tout élément de G est inversible, i.e., $\forall x \in G$, $\exists y \in G$ (unique, noté x^{-1} ou $-x$) t.q. $x \circ y = y \circ x = e$

Si $\forall x, y \in G$, $x \circ y = y \circ x$, alors groupe commutatif ou abélien.

Rappels - mise à niveau en algèbre

Définition

Si un ensemble jouit uniquement des deux premières propriétés, on dit alors qu'il s'agit d'un monoïde

Exemples

- L'ensemble $(\mathbb{Z}/m\mathbb{Z}, +)$, aussi noté $(\mathbb{Z}_m, +)$, des entiers modulo m muni de l'opération d'addition correspondante est un groupe.
- L'ensemble $(\mathbb{Q} \setminus \{0\}, \cdot)$ en est un aussi.
- L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices carrées inversibles de dimension n muni de la multiplication matricielle est un groupe non commutatif.
- Par contre, $(\mathbb{N}, +)$ est un monoïde qui n'est pas un groupe.

Rappels - mise à niveau en algèbre

Définition

Soient $(G, \circ, e_G)$ et $(H, \diamond, e_H)$ deux groupes. Un homomorphisme de groupes est une application $f : G \to H$ telle que

$$\forall x, y \in G : f(x \circ y) = f(x) \diamond f(y).$$

Propriétés

$f(e_G) = e_H$ et $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in G$.

Pour tout $x \in G$, on a $f(x) = f(x \circ e_G) = f(x) \diamond f(e_G)$.
Multiplier à gauche par $f(x)^{-1}$:
$f(x)^{-1} \diamond f(x) = f(x)^{-1} \diamond f(x) \diamond f(e_G)$ donc $e_H = f(e_G)$

pour tout $x \in G$, $f(e_G) = f(x \circ x^{-1}) = f(x) \diamond f(x^{-1}) = e_H$.

Rappels - mise à niveau en algèbre

Définition

Soient $(G, \circ, e_G)$ et $(H, \diamond, e_H)$ deux monoïdes. Un homomorphisme de monoïdes est une application $f : G \to H$ telle que

$$\forall x, y \in G : f(x \circ y) = f(x) \diamond f(y) \quad \textbf{et} \quad f(e_G) = e_H.$$

Rappels - mise à niveau en algèbre

Définition : anneau $(A, +, \cdot, 0, 1)$ ou $(A, +, \cdot)$

Un anneau : ensemble A muni de deux opérations internes et partout définies, $+$ et $\cdot$ de neutre respectif 0 et 1

- $(A, +, 0)$ est un groupe commutatif,
- $\cdot$ est associatif, i.e., $\forall x, y, z \in A$, $(x.y).z = x.(y.z)$,
- 1 neutre pour $\cdot$, i.e., $\forall x \in A$, $1.x = x.1 = x$,
- $\cdot$ est distributif par rapport à $+$,

$$\forall x, y, z \in A,\ (x + y).z = x.z + y.z \text{ et } x.(y + z) = x.y + x.z.$$

Un anneau est commutatif si $\cdot$ est commutative.

Rappels - mise à niveau en algèbre

Exemples

- L'ensemble $(\mathbb{Z}_m, +, \cdot)$ possède une structure d'anneau commutatif.
- L'ensemble $\mathbb{R}_n^n$ des matrices carrées de dimension n à coefficients réels muni des opérations usuelles d'addition et de multiplication possède une structure d'anneau (non commutatif).
- Soit $\mathbb{K}$ un champ, l'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est un anneau commutatif.

Exemple

Si $(A, +, \cdot)$ est un anneau, alors $(A, \cdot, 1)$ possède en particulier une structure de monoïde.

Rappels - mise à niveau en algèbre

Définition

Un anneau pour lequel $0 \neq 1$ et tout élément non nul possède un inverse pour $\cdot$, i.e., pour tout $x \in A \setminus \{0\}$, il existe $y \in A$ tel que $x.y = 1 = y.x$, est qualifié de corps. Si de plus, l'anneau est commutatif, on parle alors de champ

Exemples

- L'ensemble $\mathbb{Z}_p$ est un champ si et seulement si p est un nombre premier. On le note parfois $\mathbb{F}_p$.
- Le sous-ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices inversibles de $\mathbb{R}_n^n$ est un corps.

Rappels - mise à niveau en algèbre

Définition

Soient $(A, +_A, \cdot_A, 0_A, 1_A)$ et $(B, +_B, \cdot_B, 0_B, 1_B)$ deux anneaux. Un homomorphisme d'anneaux est une application $f : A \to B$ t.q.

- f homomorphisme de groupes entre $(A, +_A, 0_A)$ et $(B, +_B, 0_B)$
- f homomorphisme de monoïdes entre $(A, \cdot_A, 1_A)$ et $(B, \cdot_B, 1_B)$.

Autrement dit, on a

$$\forall x, y \in A,\ f(x+y) = f(x) + f(y),\ f(x.y) = f(x).f(y)$$

et $f(1_A) = 1_B$.

Rappels - mise à niveau en algèbre

Définition

Soit $\mathbb{K}$ un champ (ou simplement un corps). Un espace vectoriel E sur $\mathbb{K}$ ou $\mathbb{K}$-vectoriel est un ensemble E muni d'une addition interne $+ : E \times E \to E$ et d'une multiplication interne $\cdot : \mathbb{K} \times E \to E$ tel que

- $(E, +)$ est un groupe commutatif

et pour tous $x, y \in E$ et tous $\lambda, \mu \in \mathbb{K}$

- $\lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$,
- $1 \cdot x = x$,
- $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$,
- $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$.

Si $\mathbb{K}$ n'est pas un champ, mais simplement un anneau, on parle alors de $\mathbb{K}$-module.

Rappels - mise à niveau en algèbre

Suite...

Un espace vectoriel est de dimension finie s'il contient une partie génératrice finie.

Sa dimension est alors le nombre d'éléments d'une de ses bases.

Remarque

Un A-module ne possède pas toujours de base.

EXTENSION DE CHAMP

Soient $\mathbb{K}, \mathbb{L}$ deux champs tels que $\mathbb{K}$ soit un sous-champ de $\mathbb{L}$.

$\mathbb{L}$ est une extension de champ de $\mathbb{K}$.

$\mathbb{L}$ est un $\mathbb{K}$-vectoriel.

Si la dimension de $\mathbb{L}$ comme $\mathbb{K}$-vectoriel est finie et égale à d, on parle d'extension finie et d = degré de l'extension, $[\mathbb{L} : \mathbb{K}]$

Plus généralement, si $\mathbb{K}$ et $\mathbb{L}$ sont deux champs et s'il existe un plongement $h : \mathbb{K} \to \mathbb{L}$ (i.e., un homomorphisme injectif), alors on dit que $\mathbb{L}$ est une extension de $\mathbb{K}$ car $\mathbb{K}$ est isomorphe à un sous-champ de $\mathbb{L}$.

REMARQUE

Si $\mathbb{K}$ est un champ fini contenant t éléments et si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré fini d, alors $\mathbb{L}$ contient t^d éléments.

Il existe une base $(\ell_1, \ldots, \ell_d)$ de $\mathbb{L}$

tout élément de $\mathbb{L}$ se décompose de manière unique comme

$$k_1\ell_1 + \cdots + k_d\ell_d$$

avec les $k_i \in \mathbb{K}$.

EXEMPLE - EXTENSION DE CHAMP

$\mathbb{Q}(\sqrt{2})$ = {expr. rationnelles avec $\sqrt{2}$ et des éléments de $\mathbb{Q}$ } plus petit champ contenant $\mathbb{Q}$ et $\sqrt{2}$

$$\frac{\sum_{i=0}^{m} q_i (\sqrt{2})^i}{\sum_{j=0}^{n} r_j (\sqrt{2})^j}, \quad q_i, r_j \in \mathbb{Q}, m, n \in \mathbb{N}.$$

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

$(1, \sqrt{2})$ base de $\mathbb{Q}(\sqrt{2})$ vu comme $\mathbb{Q}$-vectoriel, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Par des raisonnements analogues,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$$

et $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

DÉFINITION

Un idéal (bilatère) d'un anneau $(A, +, \cdot)$ est un sous-ensemble $I \subset A$ tel que

- $(I, +, 0)$ est un groupe commutatif,
- pour tous $i \in I$ et $a \in A$, $a.i$ et $i.a$ appartiennent à I.

DÉFINITION

Soient $a_1, \ldots, a_k$ des éléments de A. Dans le cas où A est un anneau commutatif, l'idéal engendré par $a_1, \ldots, a_k$ est

$$\langle a_1, \ldots, a_k \rangle = \left\{ \sum_{i=1}^{k} b_i a_i \mid b_i \in A \right\}.$$

RAPPELS - MISE À NIVEAU EN ALGÈBRE

DÉFINITION

Un idéal engendré par un unique élément $a \in A$, i.e.,

$$I = \langle a \rangle$$

est qualifié de principal.

Un anneau principal est un anneau intègre dans lequel tout idéal est principal.

DÉFINITION

Un idéal I d'un anneau A est maximal si I est propre, i.e., $I \neq A$, et s'il n'est contenu strictement dans aucun idéal propre, i.e., si J est un idéal tel que $I \subsetneq J$, alors $J = A$.

RAPPELS - MISE À NIVEAU EN ALGÈBRE

EXEMPLE

Si $\mathbb{K}$ est un champ, les seuls idéaux de $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$.

si $a \neq 0$ appartient à un idéal $I \neq \{0\}$, alors $a^{-1}.a = 1 \in I$ et de là, tout élément de $\mathbb{K}$ appartient à I.

EXEMPLE

Les idéaux de $\mathbb{Z}$ sont les $m\mathbb{Z} = \langle m \rangle$ et $\mathbb{Z}$ est donc un anneau principal.

RAPPELS - MISE À NIVEAU EN ALGÈBRE

DÉFINITION - QUOTIENT D'UN ANNEAU PAR UN IDÉAL

$(A, +, \cdot, 0, 1)$ anneau et I idéal de A.

I est un sous-groupe du groupe commutatif $(A, +, 0)$, on peut considérer le groupe quotient A/I

les éléments de A/I sont les classes de la forme

$$a + I = \{a + i \mid i \in I\}, \quad a \in A.$$

La somme de deux classes $a + I$ et $b + I$ est la classe

$$(a + b) + I$$

Le neutre : la classe

$$0 + I = I$$

RAPPELS - MISE À NIVEAU EN ALGÈBRE

DÉFINITION - QUOTIENT D'UN ANNEAU PAR UN IDÉAL

On munit A/I d'une structure d'anneau :

le produit des classes $a + I$ et $b + I$ est la classe

$$(a.b) + I$$

le neutre est

$$1 + I$$

La projection canonique $\pi : A \to A/I : a \mapsto a + I$ est alors un homomorphisme d'anneaux.

EXEMPLE

L'anneau quotient de $\mathbb{Z}$ par l'idéal $m\mathbb{Z}$ est l'anneau $\mathbb{Z}_m$.
Une classe est un élément de la forme $a + \langle m \rangle$.

Pour $m = 3$, on a par exemple,

$$(1 + \langle 3 \rangle) + (2 + \langle 3 \rangle) = 3 + \langle 3 \rangle = 0 + \langle 3 \rangle$$

et

$$(2 + \langle 3 \rangle).(2 + \langle 3 \rangle) = 4 + \langle 3 \rangle = 1 + \langle 3 \rangle.$$

Dans $\mathbb{Z}_m$,

$$\forall a, b \in \mathbb{Z} : \ a + \langle m \rangle = b + \langle m \rangle \Leftrightarrow a \equiv b \pmod{m}.$$

REMARQUE

Un élément $a + I$ de A/I est nul (i.e., correspond au neutre pour l'addition dans l'anneau quotient) SSI $a \in I$.

$$a + I = \{a + i \mid i \in I\} = I \Leftrightarrow a \in I$$

THÉORÈME

Soient A un anneau commutatif et I un idéal de A.

L'anneau quotient A/I est un champ si et seulement si I est un idéal maximal.

IDÉAUX ET DIVISIBILITÉ

Soient A un anneau principal (muni d'une division euclidienne) et $a, b \in A \setminus \{0\}$. On a

- $\langle a \rangle \supset \langle b \rangle$ SSI a divise b.
- $\langle a \rangle = \langle b \rangle$ SSI $a = ub$ avec u inversible dans A.

RAPPEL

Si $a = ub$ avec u inversible, a et b associés

$\mathbb{K}$ est un champ.

DÉFINITION

Un polynôme à coeff. dans $\mathbb{K}$ est une suite $(\alpha_n)_{n \in \mathbb{N}}$ d'éléments de $\mathbb{K}$ non tous nuls t.q. $\exists d \geq 0$ t.q. $\alpha_n = 0$ pour tout $n > d$.

$$P = \sum_{i=0}^{d} \alpha_i X^i = \alpha_d X^d + \cdots + \alpha_1 X + \alpha_0, \quad \alpha_d \neq 0$$

d : degré, $\deg P$.

La valeur $P(\beta)$ de ce polynôme évalué en $\beta \in \mathbb{K}$ est

$$P(\beta) = \sum_{i=0}^{d} \alpha_i \beta^i = \alpha_d \beta^d + \cdots + \alpha_1 \beta + \alpha_0.$$

RAPPELS - MISE À NIVEAU EN ALGÈBRE

TERMINOLOGIE

La suite nulle est appelé polynôme nul.

Si $\alpha_d = 1$, polynôme monique (ou unitaire).

Si $d = 0$, le polynôme est constant.

STRUCTURE ALGÉBRIQUE

L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ possède alors une structure d'anneau.

POLYNÔME $\neq$ FONCTION POLYNOMIALE

sur $\mathbb{Z}_3[X]$, $P(X) = X^2 + 1$ et $Q(X) = X^3 + X^2 - X + 1$ sont distincts mais représentent la même fonction : $\forall z \in \mathbb{Z}_3$, $P(z) = Q(z)$

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Il est aisé de munir $\mathbb{K}[X]$ de la divison euclidienne (calcul écrit comme dans $\mathbb{C}[z]$)

THÉORÈME

Soit $\mathbb{K}$ un champ. Si $D \in \mathbb{K}[X]$ est non nul, alors pour tout $P \in \mathbb{K}[X]$, il existe des polynômes uniques Q et R tels que

$$P = Q.D + R, \quad \text{avec } \deg R < \deg D.$$

REMAQUE

Si $\mathbb{K}$ n'est pas un champ mais simplement un anneau, pour assurer l'existence des polynômes Q et R, il faut que le coefficient principal de D soit inversible.

l'unicité de Q et R n'est assurée que si l'anneau est intègre.

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Si $P = Q.R$, alors le polynôme Q divise le polynôme P.

PROPRIÉTÉ

Puisque $\mathbb{K}$ est un champ

$$\deg P.Q = \deg P + \deg Q$$

donc $\mathbb{K}[X]$ est un anneau intègre.
$P.Q = 0$ entraîne $P = 0$ ou $Q = 0$.

REMARQUE

Si $\mathbb{K}$ est simplement un anneau, dans $\mathbb{Z}_4[X]$,

$$(2X^2 + 1).(2X + 1) = 2X^2 + 2X + 1$$

$\mathbb{Z}_4[X]$ n'est pas intègre.

RAPPELS - MISE À NIVEAU EN ALGÈBRE

DÉFINITION

Un polynôme non constant P est irréductible si $P = Q.R$ entraîne que Q ou R est constant.

P ne peut pas s'écrire comme le produit de deux polynômes de degré strictement inférieur au degré de P.

En particulier, tout polynôme de degré 1 est irréductible.

EXEMPLE

Le polynôme $X^2 + 1$ est irréductible sur $\mathbb{R}[X]$ mais pas sur $\mathbb{C}[X]$

RAPPELS - MISE À NIVEAU EN ALGÈBRE

REMARQUES

Dans $\mathbb{K}[X]$, les seuls éléments inversibles sont les polynômes constants $k \in \mathbb{K} \setminus \{0\}$.

Si P est de deg≥ 1, alors pour tout $Q \in \mathbb{K}[X]$, deg $P.Q \geq 1$ et P n'est pas inversible.

$\langle P \rangle = \mathbb{K}[X]$ SSI $P \neq 0$ est constant.

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Une conséquence de la division euclidienne...

THÉORÈME

Soit $\mathbb{K}$ un champ. L'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est principal.

COROLLAIRE

Soient $\mathbb{K}$ un champ et $P \in \mathbb{K}[X]$.

L'idéal $\langle P \rangle$ est un idéal maximal SSI P est irréductible.

Démonstration ...

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Nous pouvons construire des champs finis...

Ingrédient 1

THÉORÈME

Soient A un anneau commutatif et I un idéal de A.
L'anneau quotient A/I est un champ SSI I est un idéal maximal.

Ingrédient 2

COROLLAIRE

Soient $\mathbb{K}$ un champ et $P \in \mathbb{K}[X]$.
L'idéal $\langle P \rangle$ est un idéal maximal SSI P est irréductible.

PROPOSITION

Soit $\mathbb{K}$ un champ. L'anneau quotient $\mathbb{K}[X]/\langle P \rangle$ est un champ SSI P est un polynôme irréductible.

RAPPELS - MISE À NIVEAU EN ALGÈBRE

EXEMPLE

$\mathbb{Z}_3[X]$ quotienté par l'idéal $\langle X^2 + 1 \rangle$.

$X^2 + 1$ irréductible sur $\mathbb{Z}_3[X]$?

$$1,\ 2,\ X,\ X+1,\ X+2,\ 2X,\ 2x+1,\ 2X+2$$

Les classes de l'anneau quotient sont de la forme

$$P + \langle X^2 + 1 \rangle, \quad \deg P < 2$$

car pour tous $P, Q \in \mathbb{K}[X]$, $P + \langle X^2 + 1 \rangle = Q + \langle X^2 + 1 \rangle$
SSI P et Q ont même reste après division par $X^2 + 1$.

Notons $P + \langle X^2 + 1 \rangle$ simplement P.

EXEMPLE

$\mathbb{Z}_3[X]$ quotienté par l'idéal $\langle X^2+1\rangle$.

X^2+1 irréductible sur $\mathbb{Z}_3[X]$?

$$1,\ 2,\ X,\ X+1,\ X+2,\ 2X,\ 2x+1,\ 2X+2$$

Les classes de l'anneau quotient sont de la forme

$$P+\langle X^2+1\rangle, \quad \deg P<2$$

car pour tous $P, Q \in \mathbb{K}[X]$, $P+\langle X^2+1\rangle = Q+\langle X^2+1\rangle$
SSI P et Q ont même reste après division par X^2+1.

Notons $P+\langle X^2+1\rangle$ simplement P.

RAPPELS - MISE À NIVEAU EN ALGÈBRE

EXEMPLE

$\mathbb{Z}_3[X]$ quotienté par l'idéal $\langle X^2+1\rangle$.

X^2+1 irréductible sur $\mathbb{Z}_3[X]$?

$$1,\ 2,\ X,\ X+1,\ X+2,\ 2X,\ 2x+1,\ 2X+2$$

Les classes de l'anneau quotient sont de la forme

$$P+\langle X^2+1\rangle, \quad \deg P<2$$

car pour tous $P, Q \in \mathbb{K}[X]$, $P+\langle X^2+1\rangle = Q+\langle X^2+1\rangle$
SSI P et Q ont même reste après division par X^2+1.

Notons $P+\langle X^2+1\rangle$ simplement P.

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Table de multiplication (sans 0) — version 1

·	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
1	1	2	X	$X+1$	$X+2$	$2X$	$2X+1$	$2X+2$
2	2	1	$2X$	$2X+2$	$2X+1$	X	$X+2$	$X+1$
X	X	$2X$	2	$X+2$	$2X+2$	1	$X+1$	$2X+1$
$X+1$	$X+1$	$2X+2$	$X+2$	$2X$	1	$2X+1$	2	X
$X+2$	$X+2$	$2X+1$	$2X+2$	1	X	$X+1$	$2X$	1
$2X$	$2X$	X	1	$2X+1$	$X+1$	2	$2X+2$	$X+2$
$2X+1$	$2X+1$	$X+2$	$X+1$	2	$2X$	$2X+2$	X	1
$2X+2$	$2X+2$	$X+1$	$2X+1$	X	2	$X+2$	1	$2X$

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Table de multiplication (sans 0)

version 2 (liste des coefficients)

·	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)	(2, 0)	(2, 1)	(2, 2)
(0, 1)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)	(2, 0)	(2, 1)	(2, 2)
(0, 2)	(0, 2)	(0, 1)	(2, 0)	(2, 2)	(2, 1)	(1, 0)	(1, 2)	(1, 1)
(1, 0)	(1, 0)	(2, 0)	(0, 2)	(1, 2)	(2, 2)	(0, 1)	(1, 1)	(2, 1)
(1, 1)	(1, 1)	(2, 2)	(1, 2)	(2, 0)	(0, 1)	(2, 1)	(0, 2)	(1, 0)
(1, 2)	(1, 2)	(2, 1)	(2, 2)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(0, 1)
(2, 0)	(2, 0)	(1, 0)	(0, 1)	(2, 1)	(1, 1)	(0, 2)	(2, 2)	(1, 2)
(2, 1)	(2, 1)	(1, 2)	(1, 1)	(0, 2)	(2, 0)	(2, 2)	(1, 0)	(0, 1)
(2, 2)	(2, 2)	(1, 1)	(2, 1)	(1, 0)	(0, 2)	(1, 2)	(0, 1)	(2, 0)

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Version 3 : En base 3...
$(x_{f-1}, \ldots, x_0) \in (\mathbb{Z}_p)^f$ correspond à l'entier

$$\sum_{i=0}^{f-1} x_i \, p^i.$$

·	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	6	8	7	3	5	4
3	3	6	2	5	8	1	4	7
4	4	8	5	6	1	7	2	3
5	5	7	8	1	3	4	6	1
6	6	3	1	7	4	2	8	5
7	7	5	4	2	6	8	3	1
8	8	4	7	3	2	5	1	6

RAPPELS - MISE À NIVEAU EN ALGÈBRE

"Mathematica crash course"

```
In[71]:= Table[i, {i, 1, 4}]
Out[71]= {1, 2, 3, 4}

In[72]:= Table[i + j^2, {i, 1, 3}, {j, 1, 2}]
Out[72]= {{2, 5}, {3, 6}, {4, 7}}

In[73]:= CoefficientList[X^3 + 2 X - 1, X]
Out[73]= {-1, 2, 0, 1}

In[74]:= Reverse[CoefficientList[X^3 + 2 X - 1, X]]
Out[74]= {1, 0, 2, -1}

In[86]:= PadLeft[{1, 2, 3}, 5]
Out[86]= {0, 0, 1, 2, 3}

In[87]:= IntegerDigits[1324, 3]
Out[87]= {1, 2, 1, 1, 0, 0, 1}

In[88]:= FromDigits[{1, 2, 1, 1, 0, 0, 1}, 3]
Out[88]= 1324

In[90]:= {1, 2, 1, 1, 0, 0, 1}.Reverse[Table[3^i, {i, 0, 6}]]
Out[90]= 1324
```

RAPPELS - MISE À NIVEAU EN ALGÈBRE

"Mathematica crash course"

```
In[81]:= PolynomialMod[4 X^3 + X - 1, X^2 - 1]
Out[81]= -1 + 5 X

In[82]:= PolynomialQuotient[4 X^3 + X - 1, X^2 - 1, X]
Out[82]= 4 X

In[83]:= Expand[4 X (X^2 - 1) + (-1 + 2 X)]
Out[83]= -1 - 2 X + 4 X^3

In[84]:= PolynomialMod[4 X^3 + X - 1, X^2 - 1, Modulus → 3]
Out[84]= 2 + 2 X

In[85]:= PolynomialMod[4 X^3 + X - 1, X^2 - 1, Modulus → 2]
Out[85]= 1 + X
```

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Avec `Mathematica`

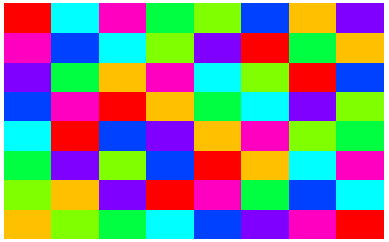
```
In[1]:= t = {1, 2, X, X + 1, X + 2, 2 X, 2 X + 1, 2 X + 2}
Out[1]= {1, 2, X, 1 + X, 2 + X, 2 X, 1 + 2 X, 2 + 2 X}

In[29]:= tab = Table[
           PolynomialMod[t[[i]] t[[j]], X^2 + 1, Modulus → 3],
           {i, 1, 8}, {j, 1, 8}]
Out[29]= {{1, 2, X, 1 + X, 2 + X, 2 X, 1 + 2 X, 2 + 2 X}, {2, 1, 2 X, 2 + 2 X, 1 + 2 X, X, 2 + X, 1 + X},
          {X, 2 X, 2, 2 + X, 2 + 2 X, 1, 1 + X, 1 + 2 X}, {1 + X, 2 + 2 X, 2 + X, 2 X, 1, 1 + 2 X, 2, X},
          {2 + X, 1 + 2 X, 2 + 2 X, 1, X, 1 + X, 2 X, 2}, {2 X, X, 1, 1 + 2 X, 1 + X, 2, 2 + 2 X, 2 + X},
          {1 + 2 X, 2 + X, 1 + X, 2, 2 X, 2 + 2 X, X, 1}, {2 + 2 X, 1 + X, 1 + 2 X, X, 2, 2 + X, 1, 2 X}}
```

Avec Mathematica

```
In[28]:= Table[
          PadLeft[
           Reverse[CoefficientList[
             PolynomialMod[t[[i]] t[[j]], X^2 + 1, Modulus → 3]
             , X]]
           , 2],
          {i, 1, 8}, {j, 1, 8}]

Out[28]= {{{0, 1}, {0, 2}, {1, 0}, {1, 1}, {1, 2}, {2, 0}, {2, 1}, {2, 2}},
          {{0, 2}, {0, 1}, {2, 0}, {2, 2}, {2, 1}, {1, 0}, {1, 2}, {1, 1}},
          {{1, 0}, {2, 0}, {0, 2}, {1, 2}, {2, 2}, {0, 1}, {1, 1}, {2, 1}},
          {{1, 1}, {2, 2}, {1, 2}, {2, 0}, {0, 1}, {2, 1}, {0, 2}, {1, 0}},
          {{1, 2}, {2, 1}, {2, 2}, {0, 1}, {1, 0}, {1, 1}, {2, 0}, {0, 2}},
          {{2, 0}, {1, 0}, {0, 1}, {2, 1}, {1, 1}, {0, 2}, {2, 2}, {1, 2}},
          {{2, 1}, {1, 2}, {1, 1}, {0, 2}, {2, 0}, {2, 2}, {1, 0}, {0, 1}},
          {{2, 2}, {1, 1}, {2, 1}, {1, 0}, {0, 2}, {1, 2}, {2, 1}, {0, 1}}}

In[30]:= Table[
          FromDigits[
           Reverse[CoefficientList[PolynomialMod[t[[i]] t[[j]], X^2 + 1, Modulus → 3], X]]
           , 3],
          {i, 1, 8}, {j, 1, 8}]

Out[30]= {{1, 2, 3, 4, 5, 6, 7, 8}, {2, 1, 6, 8, 7, 3, 5, 4},
          {3, 6, 2, 5, 8, 1, 4, 7}, {4, 8, 5, 6, 1, 7, 2, 3}, {5, 7, 8, 1, 3, 4, 6, 2},
          {6, 3, 1, 7, 4, 2, 8, 5}, {7, 5, 4, 2, 6, 8, 3, 1}, {8, 4, 7, 3, 2, 5, 1, 6}}
```


Avec Mathematica

```
In[31]:= m = Table[Hue[
             FromDigits[Reverse[
               CoefficientList[PolynomialMod[t[[i]] t[[j]], X^2 + 1, Modulus → 3], X]], 3]
             / 8],
           {i, 1, 8}, {j, 1, 8}];

In[32]:= Show[Graphics[RasterArray[m]]]
```



```
Out[32]= - Graphics -
```


"Mathematica crash course"

```
In[16]:= Table[IntegerDigits[n, 2], {n, 1, 10}]

Out[16]= {{1}, {1, 0}, {1, 1}, {1, 0, 0}, {1, 0, 1},
          {1, 1, 0}, {1, 1, 1}, {1, 0, 0, 0}, {1, 0, 0, 1}, {1, 0, 1, 0}}

In[17]:= TableForm[%]

Out[17]//TableForm=
1
1  0
1  1
1  0  0
1  0  1
1  1  0
1  1  1
1  0  0  0
1  0  0  1
1  0  1  0

In[18]:= Table[PadLeft[IntegerDigits[n, 2], 5], {n, 1, 10}]

Out[18]= {{0, 0, 0, 0, 1}, {0, 0, 0, 1, 0}, {0, 0, 0, 1, 1}, {0, 0, 1, 0, 0}, {0, 0, 1, 0, 1},
          {0, 0, 1, 1, 0}, {0, 0, 1, 1, 1}, {0, 1, 0, 0, 0}, {0, 1, 0, 0, 1}, {0, 1, 0, 1, 0}}

In[19]:= Table[PadLeft[IntegerDigits[n, 2], 5].{X^4, X^3, X^2, X, 1}, {n, 1, 10}]

Out[19]= {1, X, 1 + X, X^2, 1 + X^2, X + X^2, 1 + X + X^2, X^3, 1 + X^3, X + X^3}
```

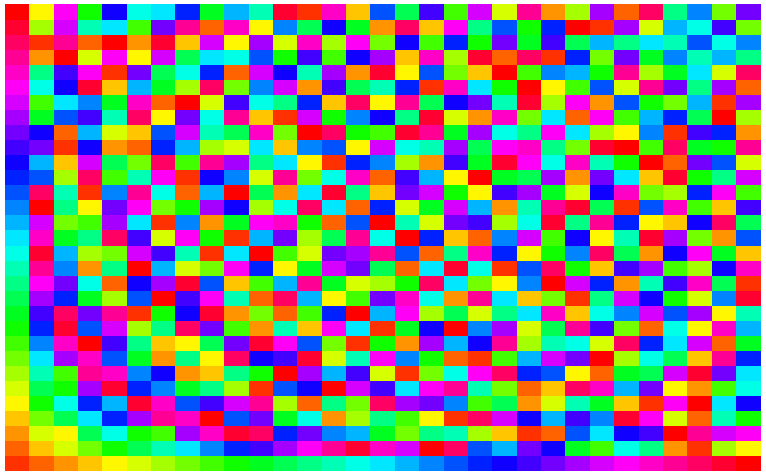

UN AUTRE EXEMPLE

$1 + X + X^3 + X^4 + X^5$ irréductible sur $\mathbb{Z}_2[X]$

$$\mathbb{Z}_2[X]/\langle 1 + X + X^3 + X^4 + X^5 \rangle$$

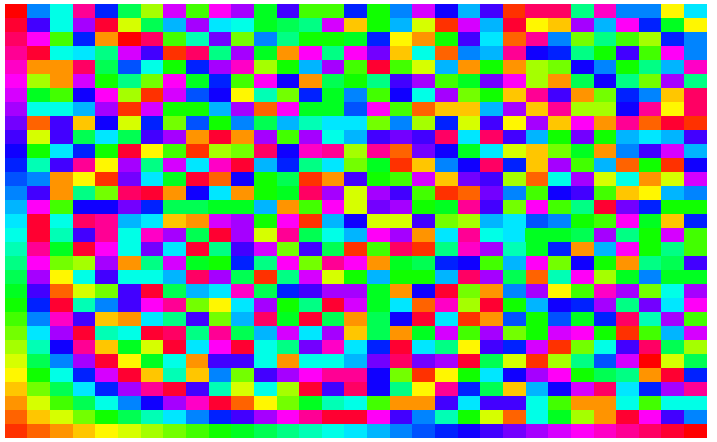
```
In[64]:= t = Table[PadLeft[IntegerDigits[n, 2], 5].{X^4, X^3, X^2, X, 1}, {n, 1, 31}]

Out[64]= {1, X, 1 + X, X^2, 1 + X^2, X + X^2, 1 + X + X^2, X^3, 1 + X^3, X + X^3, 1 + X + X^3,
          X^2 + X^3, 1 + X^2 + X^3, X + X^2 + X^3, 1 + X + X^2 + X^3, X^4, 1 + X^4, X + X^4, 1 + X + X^4,
          X^2 + X^4, 1 + X^2 + X^4, X + X^2 + X^4, 1 + X + X^2 + X^4, X^3 + X^4, 1 + X^3 + X^4, X + X^3 + X^4,
          1 + X + X^3 + X^4, X^2 + X^3 + X^4, 1 + X^2 + X^3 + X^4, X + X^2 + X^3 + X^4, 1 + X + X^2 + X^3 + X^4}

In[65]:= tab = Table[
            PolynomialMod[t[[i]] t[[j]], 1 + X + X^3 + X^4 + X^5, Modulus → 2],
            {i, 1, 31}, {j, 1, 31}]
```

RAPPELS - MISE À NIVEAU EN ALGÈBRE



RAPPELS - MISE À NIVEAU EN ALGÈBRE

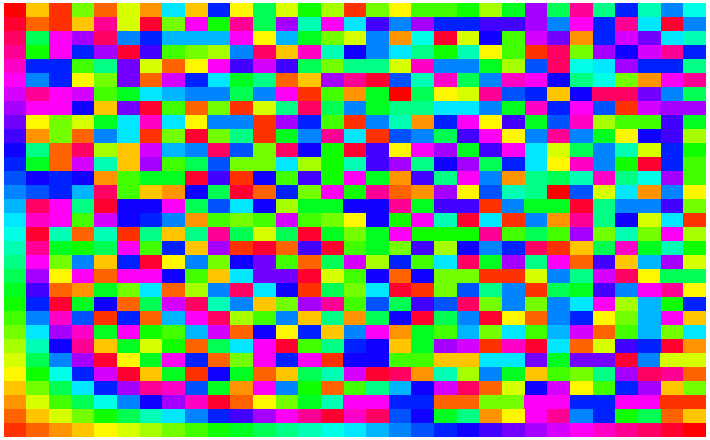
Isomorphisme avec $\mathbb{Z}_2[X]/\langle 1+X+X^2+X^3+X^5\rangle$?



Patience... (Structure des corps finis)

RAPPELS - MISE À NIVEAU EN ALGÈBRE

ou encore isomorphisme avec $\mathbb{Z}_2[X]/\langle 1+X^2+X^3+X^4+X^5\rangle$?

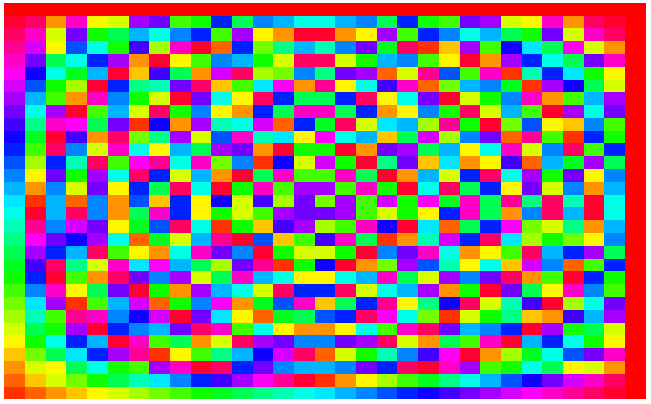


RAPPELS - MISE À NIVEAU EN ALGÈBRE

Et si on considère un polynôme réductible ?

EXEMPLE

Dans $\mathbb{Z}_2[X]$, $X^5+1=(X^4+X^3+X^2+X+1)(X+1)$

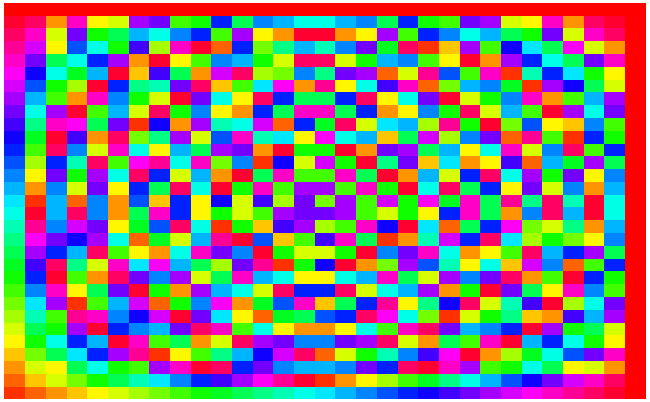


RAPPELS - MISE À NIVEAU EN ALGÈBRE

Et si on considère un polynôme réductible ?

EXEMPLE

Dans $\mathbb{Z}_2[X]$, $X^5+1=(X^4+X^3+X^2+X+1)(X+1)$



RAPPELS - MISE À NIVEAU EN ALGÈBRE

Dans la table de multiplication d'un corps

sur chaque ligne/colonne, permutation des éléments

$$x.y = x.z \Rightarrow y = z$$

```
In[79]:= Table[
          FromDigits[
           Reverse[CoefficientList[PolynomialMod[t[[i]] t[[j]], X^5 + 1, Modulus → 2], X]]
           , 2],
          {i, 3, 3}, {j, 1, 31}]

Out[79]= {{3, 6, 5, 12, 15, 10, 9, 24, 27, 30, 29, 20, 23,
           18, 17, 17, 18, 23, 20, 29, 30, 27, 24, 9, 10, 15, 12, 5, 6, 3, 0}}

In[80]:= m = Map[Hue[# / 31] &, %, {2}]

Out[80]= {{Hue[3/31], Hue[6/31], Hue[5/31], Hue[12/31], Hue[15/31], Hue[10/31], Hue[9/31], Hue[24/31],
           Hue[27/31], Hue[30/31], Hue[29/31], Hue[20/31], Hue[23/31], Hue[18/31], Hue[17/31], Hue[17/31],
           Hue[18/31], Hue[23/31], Hue[20/31], Hue[29/31], Hue[30/31], Hue[27/31], Hue[24/31],
           Hue[9/31], Hue[10/31], Hue[15/31], Hue[12/31], Hue[5/31], Hue[6/31], Hue[3/31], Hue[0]}}

In[78]:= Show[Graphics[RasterArray[m]]]
```

RAPPELS - MISE À NIVEAU EN ALGÈBRE

EN RÉSUMÉ

Si p est un nombre premier et si P un polynôme irréductible de degré f de $\mathbb{Z}_p[X]$, alors

$$\boxed{\mathbb{Z}_p[X]/\langle P\rangle}$$

est un champ à p^f éléments.

Questions :

- existence de polynômes irréductibles ?
- nombre d'éléments d'un champ fini quelconque ?

RAPPELS - MISE À NIVEAU EN ALGÈBRE

Nous devons encore démontrer le résultat suivant :

COROLLAIRE

Soient $\mathbb{K}$ un champ et $P \in \mathbb{K}[X]$. L'idéal $\langle P\rangle$ est un idéal maximal si et seulement si P est irréductible.

$\Rightarrow$ Supposons $\langle P\rangle$ idéal maximal avec $P \neq 0$.

P ne peut pas être constant.
P.A. Supposons qu'il le soit. $P = k \in \mathbb{K}\setminus\{0\}$ et $k^{-1}.k = 1$ doit appartenir à $\langle k\rangle$ d'où $\langle P\rangle = \mathbb{K}[X]$, impossible !

Supposons à présent que P est un polynôme non constant qui se factorise en $P = Q.R$.

$\langle P\rangle \subseteq \langle Q\rangle$. Si $\langle P\rangle = \langle Q\rangle$, alors R est constant. Sinon, $\langle P\rangle \subsetneq \langle Q\rangle$ et puisque $\langle P\rangle$ est maximal, $\langle Q\rangle = \mathbb{K}[X]$ donc Q est constant.

$\Leftarrow$ si P est un polynôme irréductible,
montrer que l'anneau $\mathbb{K}[X]/\langle P\rangle$ est un champ
(d'où conclusion, par thm...).

Thèse : tout élément non nul $\pi(Q) = Q + \langle P\rangle$ du quotient $\mathbb{K}[X]/\langle P\rangle$ est inversible.

REM : $\pi(Q)$ est non nul SSI $Q \notin \langle P\rangle$.

Partie 1. Montrons que $\langle P, Q\rangle = \mathbb{K}[X]$.

Puisque $\mathbb{K}[X]$ est principal, $\exists T$ t.q. $\langle P, Q\rangle = \langle T\rangle$.

$\exists\ U$ et V t.q. $P = U.T$ et $Q = V.T$.

Par hypothèse, P irréductible, donc U ou T est constant.

Si T constant, alors $\langle P, Q\rangle = \langle T\rangle = \mathbb{K}[X]$.
Si U constant, $U = k \in \mathbb{K}$, $k \neq 0$, U inversible dans $\mathbb{K}[X]$
P et T sont associés, $\langle P\rangle = \langle T\rangle = \langle P, Q\rangle$, $Q \in \langle P\rangle$, impossible !

Partie 2. Nous savons que $\langle P, Q\rangle = \mathbb{K}[X]$.

$\langle P, Q\rangle = \mathbb{K}[X] \ni 1$. $\exists\ A, B \in \mathbb{K}[X]$ t.q.

$$1 = A.P + B.Q.$$

Dans l'anneau quotient $\mathbb{K}[X]/\langle P\rangle$,

$$(B + \langle P\rangle).(Q + \langle P\rangle) = 1 + \langle P\rangle$$

et donc, $\pi(Q)$ est inversible d'inverse $B + \langle P\rangle$. **QED**

PROPOSITION

Tout polynôme de $\mathbb{K}[X]$ se décompose de manière unique comme produit de polynômes irréductibles (à des facteurs constants et à l'ordre des facteurs près).

$\deg P.Q = \deg P + \deg Q \Rightarrow$ existence de la décomposition
si un polynôme n'est pas irréductible,
il se factorise en un produit de 2 polynômes de degré <
la procédure s'arrête.

L'unicité de la décomposition découle du lemme suivant.

LEMME

Si $P \in \mathbb{K}[X]$ est irréductible et si P divise $F.G$,
alors P divise F ou G.

LEMME

Si $P \in \mathbb{K}[X]$ est irréductible et si P divise $F.G$,
alors P divise F ou G.

Si P ne divise pas F. $F \notin \langle P\rangle$

$\langle P\rangle$ inclus strictement dans $\langle P, F\rangle$.

Puisque P irréductible, $\langle P\rangle$ est maximal.

Donc, $\langle P, F\rangle = \mathbb{K}[X]$ contient 1
$\exists\ S$ et T t.q. $1 = S.P + T.F$.

$$G = SPG + TFG$$

P divise chacun des deux termes de la somme, P divise G.
QED

Rappels - mise à niveau en algèbre

Remarque

les polynômes irréductibles jouent, dans $\mathbb{K}[X]$, le même rôle que les nombres premiers, dans l'ensemble des entiers.

A suivre...

moyen commode pour générer des champs finis à p^f éléments pour tout $p \geq 2$ premier,

s'il existe au moins un polynôme irréductible de degré f sur $\mathbb{Z}_p$.

Dans la suite, construction alternative en considérant l'extension d'un champ $\mathbb{K}$ par un élément algébrique

Mathématiques discrètes (2)

Michel Rigo

http://www.discmath.ulg.ac.be/

Année 2007–2008

Extension par un élément algébrique

Hypothèse de travail

$\mathbb{K}$, $\mathbb{L}$ deux champs, $\mathbb{L}$ extension de $\mathbb{K}$.

Définition

$\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ si $\exists\, P \in \mathbb{K}[X]$ t.q. $P(\alpha) = 0$.

Idéal annulateur

$$\mathcal{P}_\alpha = \{P \in \mathbb{K}[X] \mid P(\alpha) = 0\}$$

$\mathbb{K}[X]$ est principal, il existe un polynôme M_α (monique) t.q.

$$\boxed{\mathcal{P}_\alpha = \{P \in \mathbb{K}[X] \mid P(\alpha) = 0\} = \langle M_\alpha \rangle.}$$

On appelle M_α le polynôme minimum de α.

Si $\alpha' \in \mathbb{L}$: $M_\alpha(\alpha') = 0$, alors α' est un conjugué de α sur $\mathbb{K}$.

Extension par un élément algébrique

Lemme

Soit $\alpha \in \mathbb{L}$ un élément algébrique sur $\mathbb{K}$ ayant M_α comme polynôme minimum.

I) Le polynôme M_α est irréductible sur $\mathbb{K}$.

II) Pour tout $P \in \mathbb{K}[X]$, $P(\alpha) = 0$ SSI M_α divise P.

III) M_α est l'unique polynôme monique de degré minimum dans $\mathbb{K}[X]$ annulé par α.

IV) Si P est un polynôme monique irréductible sur $\mathbb{K}$ annulé par α, alors $P = M_\alpha$.

Extension par un élément algébrique

i) P.A. Si $M_\alpha = P.Q$ avec $0 < \deg P, \deg Q < \deg M_\alpha$.

Alors, $M_\alpha(\alpha) = P(\alpha).Q(\alpha) = 0$ et P ou $Q \in \mathcal{P}_\alpha$.

Donc, M_α doit diviser P ou Q. Impossible vu les degrés.

ii) Immédiat.

iii) Tout polynôme monique de $\mathbb{K}[X]$ annulé par α appartient à $\mathcal{P}_\alpha$ et est donc un multiple de M_α. Par conséquent, il est soit égal à M_α soit de degré strictement supérieur.

Extension par un élément algébrique

iv) Immédiat, $\mathcal{P}_\alpha = \langle M_\alpha \rangle$

OU...

Soit P polynôme monique irréductible sur $\mathbb{K}$ annulé par α.

Division euclidienne : $P = Q.M_\alpha + R$ avec $\deg R < \deg M_\alpha$.

a) $R = 0$. Puisque P est irréductible, $Q = 1$ et $P = M_\alpha$.

b) $R \neq 0$. Alors $P(\alpha) = R(\alpha) = 0$

vu iii), impossible car $\deg R < \deg M_\alpha$.

Extension par un élément algébrique

Remarque

Si α' est un conjugué de α, alors ils ont le même polynôme minimum, i.e., $M_\alpha = M_{\alpha'}$.

$M_\alpha(\alpha') = 0$ donc $M_\alpha \in \mathcal{P}_{\alpha'} = \langle M_{\alpha'} \rangle$ (i.e., $M_{\alpha'}$ divise M_α).

Or M_α et $M_{\alpha'}$ sont 2 polynômes moniques irréductibles.

Exemple

Le nombre d'or $\tau = (1 + \sqrt{5})/2 \in \mathbb{R}$ est algébrique sur $\mathbb{Q}$ car il est racine du polynôme

$$M_\tau(X) = X^2 - X - 1$$

Son conjugué est $(1 - \sqrt{5})/2$.

Extension par un élément algébrique

Théorème

L'élément $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ SSI $[\mathbb{K}(\alpha) : \mathbb{K}]$ est fini.

En particulier, $[\mathbb{K}(\alpha) : \mathbb{K}]$ = degré du polynôme minimum de α sur $\mathbb{K}$.

La démonstration découle de quelques remarques...

Extension par un élément algébrique

Remarque

Si $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et si $\deg M_\alpha = d$,
alors tout élément de l'extension de champ $\mathbb{K}(\alpha)$ s'exprime comme combinaison linéaire à coefficients dans $\mathbb{K}$ des éléments

$$1, \alpha, \ldots, \alpha^{d-1}$$

(Autrement dit, comme un polynôme en α à coefficients dans $\mathbb{K}$ et de degré $< d$.)

Partie 1. Elément particulier de $\mathbb{K}(\alpha)$ (en fait $\in \mathbb{K}[\alpha]$)

$$P(\alpha) = \sum_{i=0}^{n} k_i \alpha^i, \quad k_i \in \mathbb{K}$$

Extension par un élément algébrique

Division euclidienne : $P(X) = Q(X).M_\alpha(X) + R(X)$, $\deg R < d$.
Evaluer cette expression en α : $P(\alpha) = R(\alpha)$. OK

Partie 2. Elément arbitraire de $\mathbb{K}(\alpha)$

$$P(\alpha).(Q(\alpha))^{-1}, \text{ avec } \deg P, \deg Q < d$$

Puisque $\deg Q < \deg M_\alpha$, $\langle M_\alpha \rangle \subsetneq \langle Q, M_\alpha \rangle$

M_α irréductible, $\langle M_\alpha \rangle$ maximal donc $\langle Q, M_\alpha \rangle = \mathbb{K}[X] \ni 1$.

De là, il existe des polynômes S, T tels que $1 = S.M_\alpha + T.Q$

Evaluant cette expression en α : $(Q(\alpha))^{-1} = T(\alpha)$

$P(\alpha).(Q(\alpha))^{-1}$ se ramène à un produit de 2 polynômes en α, conclusion vu Partie 1.

Extension par un élément algébrique

Conclusion

$(1, \alpha, \alpha^2, \ldots, \alpha^{d-1})$: partie génératrice de $\mathbb{K}(\alpha)$.

Linéairement indépendants sur $\mathbb{K}$ car sinon,

relation linéaire à coefficients dans $\mathbb{K}$ les liant
donc polynôme de degré $< d$ de $\mathbb{K}[X]$ annulé par α !

Extension par un élément algébrique

Réciproque...

Remarque

Si $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ fini, alors les $n+1$ éléments

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

sont linéairement dépendants sur $\mathbb{K}$.

$\Rightarrow$ relation linéaire à coefficients dans $\mathbb{K}$ liant ces éléments, i.e., α est algébrique sur $\mathbb{K}$.

Exemple : τ nombre d'or

$$\frac{2\tau^2 + \tau - 3}{\tau^3 + \tau^2 - \tau + 4} = \frac{10}{22}\tau - \frac{7}{22}$$

$\mathbb{Q}(\tau) = \{a\tau + b \mid a, b \in \mathbb{Q}\}$.

Extension par un élément algébrique

Proposition

L'ensemble des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est un sous-champ de $\mathbb{L}$.

Thèse : si α, β alg. sur $\mathbb{K}$, alors $\alpha+\beta$, $\alpha.\beta$, $-\alpha$ et α^{-1} aussi.

Thèse : $\alpha+\beta$, $\alpha.\beta$, $-\alpha$ et α^{-1} appartiennent à une extension de $\mathbb{K}$ de degré fini (cf. thm...).

α alg. sur $\mathbb{K}$ donc $M=\mathbb{K}(\alpha)$ extension de deg. fini de $\mathbb{K}$.

β alg. sur $\mathbb{K}$ donc alg. sur M.

donc $M'=M(\beta)$ extension de degré fini de M et $M'\subset\mathbb{L}$.

"base télescopique", $[M':\mathbb{K}]=[M':M][M:\mathbb{K}]$
donc M' extension de $\mathbb{K}$ de degré fini.

M' champ $\ni\alpha$, β, donc $M'\ni\alpha+\beta$, $\alpha.\beta$, $-\alpha$ et α^{-1}.

Extension par un élément algébrique

construire des champs finis "par extension"...

Proposition

Soient $\mathbb{L}$ extension de $\mathbb{K}$ et $\alpha\in\mathbb{L}$ algébrique sur $\mathbb{K}$.
L'anneau quotient $\mathbb{K}[X]/\langle M_\alpha\rangle$ est isomorphe à l'extension de champ $\mathbb{K}(\alpha)$.

Premier théorème d'isomorphie : "$A/\ker\Phi\cong\operatorname{Im}\Phi$"

$$\Phi:\mathbb{K}[X]\to\mathbb{L}:P\mapsto P(\alpha)$$

Φ homomorphisme d'anneaux, $\ker\Phi=\mathcal{P}_\alpha=\langle M_\alpha\rangle$ maximal.

$\mathbb{K}[X]/\ker\Phi$ est un champ $\cong\operatorname{Im}\Phi$.

pour conclure, a-t-on $\operatorname{Im}\Phi=\{P(\alpha)\mid P\in\mathbb{K}[X]\}=\mathbb{K}(\alpha)$?

Extension par un élément algébrique

$$\Phi:\mathbb{K}[X]\to\mathbb{L}:P\mapsto P(\alpha)$$

$\alpha\in\operatorname{Im}\Phi$ (prendre $P(X)=X$)
$\mathbb{K}\subset\operatorname{Im}\Phi$ (prendre $P(X)=k$, $\forall k\in\mathbb{K}$).

donc $\mathbb{K}(\alpha)\subset\operatorname{Im}\Phi$.

L'autre inclusion :
Soit $P(\alpha)$ un élément quelconque de $\operatorname{Im}\Phi$, $P\in\mathbb{K}[X]$.

$$P(\alpha)=k_0+k_1\,\alpha+\cdots+k_d\,\alpha^d,\quad k_0,\ldots,k_d\in\mathbb{K}$$

et appartient donc à $\mathbb{K}(\alpha)$!

Extension par un élément algébrique

Application

$P(X)=X^2+X+2$ irréductible sur $\mathbb{Z}_3[X]$.

Dans $\mathbb{L}=\mathbb{Z}_3[X]/\langle P\rangle$ (extension de $\mathbb{Z}_3$), $\alpha=X+\langle P\rangle$ annule P.

$$P(\alpha)=X^2+X+2+\langle P\rangle=0+\langle P\rangle$$

$\alpha\in\mathbb{L}$ algébrique sur $\mathbb{Z}_3$ avec P comme polynôme minimum.

Ainsi, $\mathbb{Z}_3(\alpha)$ est un champ à 9 éléments

$$0,\ 1,\ 2,\ \alpha,\ \alpha+1,\ \alpha+2,\ 2\alpha,\ 2\alpha+1,\ 2\alpha+2.$$

On y effectue les sommes et les produits comme dans $\mathbb{Z}_3[\alpha]$ en se rappelant que $\alpha^2+\alpha+2=0$.

Par exemple, on a $(1+2\alpha)(2+2\alpha)=\alpha^2+2=2\alpha$.

Extension par un élément algébrique

Suite...

	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
1	1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
2	2	1	2α	$2+2\alpha$	$1+2\alpha$	α	$2+\alpha$	$1+\alpha$
α	α	2α	$1+2\alpha$	1	$1+\alpha$	$2+\alpha$	$2+2\alpha$	2
$1+\alpha$	$1+\alpha$	$2+2\alpha$	1	$2+\alpha$	2α	2	α	$1+2\alpha$
$2+\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$	2α	2	$2+2\alpha$	1	α
2α	2α	α	$2+\alpha$	2	$2+2\alpha$	$1+2\alpha$	$1+\alpha$	1
$1+2\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	α	1	$1+\alpha$	2	2α
$2+2\alpha$	$2+2\alpha$	$1+\alpha$	2	$1+2\alpha$	α	1	2α	$2+\alpha$

Extension par un élément algébrique

Un autre élément

$\beta = 2X + 2 + \langle P \rangle = 2\alpha + 2$ est aussi tel que $P(\beta) = 0$.

$P(\beta) = (2X+2)^2 + 2X + 2 + 2 + \langle P \rangle = X^2 + X + 2 + \langle P \rangle = 0 + \langle P \rangle$.

On aurait également pu construire l'extension $\mathbb{Z}_3(\beta)$, isomorphe à $\mathbb{Z}_3(\alpha)$ par l'isomorphisme envoyant α sur β et laissant les éléments de $\mathbb{Z}_3$ inchangés.

Extension par un élément algébrique

Remarque

L'exemple s'adapte à un champ arbitraire $\mathbb{K}$ et à un polynôme irréductible P de $\mathbb{K}[X]$ de degré d.

Si $\mathbb{K}$ est fini et contient t éléments et si α "annule" P, alors $\mathbb{K}(\alpha)$ est un champ à t^d éléments.

Si $\mathbb{K}$ est un champ et si α et β annulent un même polynôme irréductible $P \in \mathbb{K}[X]$, alors $\mathbb{K}(\alpha)$ et $\mathbb{K}(\beta)$ sont isomorphes par l'isomorphisme envoyant α sur β et laissant les éléments de $\mathbb{K}$ inchangés.

Mathématiques discrètes (3)

Michel Rigo

http://www.discmath.ulg.ac.be/

Année 2007–2008

ULg
UNIVERSITÉ de Liège

Extension par un élément transcendant...

Rappel

Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$ algébrique sur $\mathbb{K}$.

L'anneau quotient $\mathbb{K}[X]/\langle M_\alpha \rangle$ est isomorphe à l'extension de champ $\mathbb{K}(\alpha)$.

Ceci nous a permis de construire des champs finis...

Question

Que se passe-t-il si α est transcendant ?

Extension par un élément transcendant...

Définition

Soit $\mathbb{K}$ un champ (ou un anneau intègre).

$\mathbb{K}(x)$: champ des fractions rationnelles
(ou champ des quotients) est quotient de l'ensemble

$$\{(P, Q) \mid P, Q \in \mathbb{K}[x],\ Q \neq 0\}$$

par la relation d'équivalence

$$(P, Q) \sim (P', Q') \Leftrightarrow P.Q' = P'.Q.$$

Notation (P, Q) : "$\frac{P}{Q}$".

Définition

Si $\alpha \in \mathbb{L}$ n'est pas algébrique sur $\mathbb{K}$, alors il est transcendant sur $\mathbb{K}$.

Extension par un élément transcendant...

Lemme

Soient $\mathbb{K}$ et $\mathbb{L}$ deux champs. Si $\Phi : \mathbb{K} \to \mathbb{L}$ est un homomorphisme, alors il est injectif (i.e., c'est un plongement).

Φ est un homomorphisme, $\ker \Phi$ est un idéal de $\mathbb{K}$.

Or $\mathbb{K}$ est un champ, donc $\ker \Phi = \{0\}$ ou $\mathbb{K}$.

$\Phi(1_\mathbb{K}) = 1_\mathbb{L} \neq 0_\mathbb{L}$ donc $1_\mathbb{K} \notin \ker \Phi$ et $\ker \Phi \neq \mathbb{K}$.

Rappel : Si le noyau d'une application est réduit à $\{0\}$, alors cette application est injective. **QED**

Extension par un élément transcendant...

Proposition

Soient $\mathbb{L}$ une extension de $\mathbb{K}$ et $\alpha \in \mathbb{L}$ transcendant sur $\mathbb{K}$.
Le champ $\mathbb{K}(\alpha)$ est isomorphe à $\mathbb{K}(x)$.

$$\Phi : \mathbb{K}(x) \to \mathbb{L} : (P, Q) \mapsto P(\alpha).Q(\alpha)^{-1} =: \frac{P(\alpha)}{Q(\alpha)}.$$

Φ homomorphisme donc Φ est injectif
Φ est aussi trivialement surjectif sur son image.

$\mathbb{K}(x)$ est isomorphe à $\operatorname{Im}\Phi$. Question : $\operatorname{Im}\Phi = \mathbb{K}(\alpha)$?

$\operatorname{Im}\Phi \supseteq \mathbb{K}(\alpha)$. OK. L'autre inclusion ?
Un élément quelconque de $\operatorname{Im}\Phi$:

$$(k_0 + k_1\,\alpha + \cdots + k_d\,\alpha^d).(\ell_0 + \ell_1\,\alpha + \cdots + \ell_e\,\alpha^e)^{-1},\ k_i, \ell_j \in \mathbb{K}$$

appartient bien à $\mathbb{K}(\alpha)$. OK

Racines d'un polynôme

Définition

$\alpha \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ si $P(\alpha) = 0$.

Proposition

$\alpha \in \mathbb{K}$ est une racine de P SSI $X - \alpha$ divise P.

$\Leftarrow$: OK.

$\Rightarrow$: Division euclidienne $P(X) = Q(X).(X - \alpha) + R$ avec $\deg R < 1$. $P(\alpha) = 0$ entraîne $R = 0$.

Remarque

Soit $\alpha \in \mathbb{K}$. $P(\alpha)$ = reste de la division de P par $X - \alpha$.

$P(X) = Q(X).(X - \alpha) + R$ avec $\deg R < 1$.

Racines d'un polynôme

Définition

Si $(X - \alpha)^m$ divise P et $(X - \alpha)^{m+1}$ ne divise pas P, alors α est une racine de multiplicité m.

!! différences entre $\mathbb{K}[X]$ et $\mathbb{C}[z]$!!

Remarque

La somme des multiplicités des racines de $P \leq \deg P$.

Sur $\mathbb{R}[X]$: $X^3 - X^2 + X - 1 = (X^2 + 1)(X - 1)$ une seule racine dans $\mathbb{R}$.

Remarque

$P \in \mathbb{K}[X]$ sans racine dans $\mathbb{K} \not\Rightarrow$ P irréductible.

Sur $\mathbb{R}[X]$: $(X^2 + 1)(X^2 + 2) = X^4 + 3X^2 + 2$ pas de racine réelle mais réductible.

Racines d'un polynôme

Lemme

Soit $P \in \mathbb{K}[X]$ un polynôme de degré deux ou trois. Si P n'a pas de racine dans $\mathbb{K}$, alors P est irréductible sur $\mathbb{K}$.

P.A. Supposons P réductible,

$P = Q.R$ et Q ou R de deg. 1.

Dérivation formelle

Définition

$P = k_0 + k_1 X + k_2 X^2 \cdots + k_d X^d \in \mathbb{K}[X]$.

La dérivée (formelle) de P :

$$\mathrm{D}_X P = k_1 + 2\,k_2\,X + \cdots + d\,k_d\,X^{d-1}.$$

$$\mathrm{D}_X : \mathbb{K}[X] \to \mathbb{K}[X]$$

Propriétés :

- $\mathrm{D}_X(P + Q) = \mathrm{D}_X P + \mathrm{D}_X Q$,
- $\mathrm{D}_X(P.Q) = \mathrm{D}_X P.Q + P.\mathrm{D}_X Q$,
- $\mathrm{D}_X(k.P) = k\mathrm{D}_X P$, si $k \in \mathbb{K}$.

Dérivée (formelle) d'ordre $k \geq 2$: $\mathrm{D}_X^k P = \mathrm{D}_X^{k-1}(\mathrm{D}_X P)$.

Dérivation formelle

Proposition

$\alpha \in \mathbb{K}$ est une racine de $P \in \mathbb{K}[X]$ de multiplicité ≥ 2
SSI $P(\alpha) = (\mathrm{D}_X P)(\alpha) = 0$.

$\Rightarrow$: $P = (X-\alpha)^2 Q$ donc

$$\mathrm{D}_X P = (X-\alpha)(2Q + (X-\alpha)\mathrm{D}_X Q)$$

d'où $P(\alpha) = (\mathrm{D}_X P)(\alpha) = 0$.

$\Leftarrow$: Si $P(\alpha) = 0$, alors $P = (X-\alpha)Q$ et donc

$$\mathrm{D}_X P = (X-\alpha)\mathrm{D}_X Q + Q.$$

Or $(\mathrm{D}_X P)(\alpha) = 0$ et l'on en tire $Q(\alpha) = 0$. Par conséquent,
$Q = (X-\alpha)R$ et $P = (X-\alpha)^2 R$.

Dérivation formelle

Corollaire

Soient $\mathbb{L}$ un extension du champ $\mathbb{K}$ et $\alpha \in \mathbb{L}$, un élément algébrique sur $\mathbb{K}$.
α est racine simple de son polynôme minimum M_α. (idem pour les conjugués)

Si $(\mathrm{D}_X P)(\alpha) = 0$, alors le polynôme $\mathrm{D}_X P \in \mathbb{K}[X]$ serait de degré strictement inférieur à α et annulé par α. Impossible.

Dérivation formelle

Remarque

Dans $\mathbb{C}[z]$ on dispose d'un résultat plus fort !

α racine de multiplicité m de $P \in \mathbb{C}[z]$ non nul SSI
$P(\alpha) = (\mathrm{D}_X P)(\alpha) = \cdots = (\mathrm{D}_X^{m-1} P)(\alpha) = 0$ et $(\mathrm{D}_X^m P)(\alpha) \neq 0$.

Un tel résultat n'est en général pas vrai sur un champ fini !

Sur $\mathbb{Z}_3[X]$, $X^4 - X = (X^3-1)X = (X-1)^3 X$
1 comme racine triple mais
toutes les dérivées évaluées en 1 sont nulles !

$$4X^3 - 1 = X^3 - 1,\ 3X^2 = 0,\ 0,\ 0, \ldots$$

Dépend de la caractéristique du champ $\mathbb{K}$.

Dérivation formelle

Remarque

Dans $\mathbb{C}[z]$ on dispose d'un résultat plus fort !

α racine de multiplicité m de $P \in \mathbb{C}[z]$ non nul SSI
$P(\alpha) = (\mathrm{D}_X P)(\alpha) = \cdots = (\mathrm{D}_X^{m-1} P)(\alpha) = 0$ et $(\mathrm{D}_X^m P)(\alpha) \neq 0$.

Un tel résultat n'est en général pas vrai sur un champ fini !

Sur $\mathbb{Z}_3[X]$, $X^4 - X = (X^3-1)X = (X-1)^3 X$
1 comme racine triple mais
toutes les dérivées évaluées en 1 sont nulles !

$$4X^3 - 1 = X^3 - 1,\ 3X^2 = 0,\ 0,\ 0, \ldots$$

Dépend de la caractéristique du champ $\mathbb{K}$.

Corps de rupture

Définition

$P \in \mathbb{K}[X]$ de degré d, il existe une plus petite extension de champ $\mathbb{L}$ de $\mathbb{K}$ dans laquelle P se factorise en un produit de polynômes de degré un.

P a exactement d racines dans $\mathbb{L}$ comptées avec leur multiplicité.

Cette extension est **unique** à isomorphisme près.

corps de rupture de P sur $\mathbb{K}$ (ou corps de décomposition).

Remarque

$\mathbb{L}$ est le corps de rupture de P sur $\mathbb{K}$ si $\exists \alpha_1, \ldots, \alpha_d \in \mathbb{L}$ t.q.

$$P(X) = k\,(X-\alpha_1)\cdots(X-\alpha_d) \text{ et } \mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_d).$$

Corps de rupture

On démontrera uniquement les 2 résultats suivants.

Théorème "à la Gauss-D'Alembert"

Soit $P \in \mathbb{K}[X]$. Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que P admette au moins une racine dans $\mathbb{L}$.

Corollaire

Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que P se factorise en un produit de polynômes de degré un de $\mathbb{L}[X]$.

Corps de rupture

Thèse : extension de $\mathbb{K}$ t.q. $Q \in \mathbb{K}[X]$ irréductible a une racine.

$\mathbb{K}[X]/\langle Q\rangle = \mathbb{L}$ est un champ.

$\mathbb{K}$ est isomorphe à un sous-champ de $\mathbb{L}$: $\mathbb{L}$ extension de $\mathbb{K}$ (considérer le plongement $\Phi : \mathbb{K} \to \mathbb{L} : k \mapsto k + \langle Q\rangle$).

homomorphisme canonique
$\pi : \mathbb{K}[X] \to \mathbb{L} = \mathbb{K}[X]/\langle Q\rangle : R \mapsto R + \langle Q\rangle$

$$\alpha = \pi(X) \in \mathbb{L}$$

$\mathbb{Q} \in \mathbb{K}[X]$ donc $Q \in \mathbb{L}[X]$, π est un homomorphisme d'anneaux

$$Q(\alpha) = Q(\pi(X)) = \pi(Q(X)) = 0$$

car le zéro de $\mathbb{K}[X]/\langle Q\rangle$ est $0 + \langle Q\rangle = \pi(Q)$.

Corps de rupture

Exemple

$Q = X^2 + 1$ irréductible sur $\mathbb{R}[X]$.

$$\mathbb{R}[X]/\langle X^2+1\rangle = \{a + bX + \langle X^2+1\rangle \mid a, b \in \mathbb{R}\}$$

est un champ isomorphe à $\mathbb{C} = \mathbb{R}(i)$.

Classe du quotient notée $a + bX$, alors $(a+bX).(a'+b'X)$

$$= aa' + (ab' + a'b)X + bb'X^2 = aa' - bb' + (ab' + a'b)X$$

car $bb'X^2 = bb'(X^2+1) - bb'$.

$$\Phi : \mathbb{R}[X]/\langle X^2+1\rangle \to \mathbb{C} : a + bX + \langle X^2+1\rangle \mapsto a + i\,b$$

est un isomorphisme. On retrouve la multiplication dans $\mathbb{C}$

$$(a + i\,b).(a' + i\,b') = aa' - bb' + i\,(ab' + a'b).$$

Corps de rupture

Exemple (2)

$X^2 - 2$ irréductible sur $\mathbb{Q}$, $\mathbb{Q}[X]/\langle X^2-2\rangle$ isomorphe à $\mathbb{Q}(\sqrt{2})$

Eléments du quotient notés $a + bX$, $(a+bX).(a'+b'X) =$

$$aa' + (ab' + a'b)X + bb'X^2 = aa' + 2bb' + (ab' + a'b)X$$

car $bb'X^2 = bb'(X^2-2) + 2bb'$

$$\Phi : \mathbb{Q}[X]/\langle X^2-2\rangle \to \mathbb{Q}(\sqrt{2}) : a + bX + \langle X^2-2\rangle \mapsto a + \sqrt{2}\,b$$

On retrouve la règle du produit

$$(a+b\sqrt{2}).(a'+b'\sqrt{2}) = aa' + 2bb' + \sqrt{2}(ab' + a'b).$$

Corps de rupture

Corollaire

Soit $P \in \mathbb{K}[X]$. Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que P se factorise en un produit de polynômes de degré un de $\mathbb{L}[X]$.

Récurrence sur $\deg P$ par le théorème précédent.

Pour construire cette extension, on adjoint progressivement à $\mathbb{K}$ des racines de P. L'extension obtenue est de degré fini.

Remarque

Si 2 corps de rupture sur $\mathbb{K}$ de $P \in \mathbb{K}[X]$, alors ces deux champs sont isomorphes par un isomorphisme laissant les éléments de $\mathbb{K}$ invariants et permutant les racines de P.

A isomorphisme près, il n'existe donc qu'un corps de rupture de P sur $\mathbb{K}$.

Vers les champs finis

Théorème de Wedderburn

Tout corps fini est commutatif.

Notation

$(A, +, \cdot)$ anneau.
$(A^*, \cdot)$: groupe multiplicatif des éléments inversibles dans A.

$\mathbb{F}_q$: champ contenant q éléments (ou $GF(q)$)

$$\#\mathbb{F}_q^* = q - 1$$

Vers les champs finis

Exemple

On a $\mathbb{Z}_6^* = (\{1,5\}, \cdot)$ et $\mathbb{Z}_5^* = (\{1,2,3,4\}, \cdot)$.

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Vers les champs finis

Soit $\mathbb{K}$ un champ (ou même simplement un anneau intègre).

homomorphisme caractéristique :

$$\Phi : \mathbb{Z} \to \mathbb{K} : m \mapsto \Phi(m) = \underbrace{1_{\mathbb{K}} + \cdots + 1_{\mathbb{K}}}_{m \text{ fois}} =: m.1 \quad \text{, si } m \geq 0$$

et $\Phi(m) = -\Phi(-m)$, si $m < 0$. Φ caractérisé par $\Phi(1_{\mathbb{Z}}) = 1_{\mathbb{K}}$.

$\ker \Phi$ est un idéal de $\mathbb{Z}$. $\mathbb{Z}$ est principal.

$\exists n \geq 0 : \ker \Phi = \langle n \rangle = n\mathbb{Z}$. n est la caractéristique $\mathbb{K}$.

Premier théorème d'isomorphie :

$$\mathbb{Z}/\ker \Phi \text{ isomorphe à } \operatorname{Im} \Phi \subset \mathbb{K}$$

Vers les champs finis

Si $n = 0$, alors $\ker \Phi = \{0\}$

$\mathbb{Z}/\ker \Phi = \mathbb{Z}$ s'identifie à un sous-anneau de $\mathbb{K}$.
Le plus petit champ contenant $\mathbb{Z}$ est $\mathbb{Q}$,
donc $\mathbb{K}$ contient un sous-champ $\cong \mathbb{Q}$.

Si $n = 1$, alors $\ker \Phi = \mathbb{Z}$ et $\Phi(1) = 0$.

Or Φ est un homomorphisme et $\Phi(1) = 1$.
On aurait dans $\mathbb{K}$, $0 = 1$. Impossible dans un champ.

Si $n > 1$, $\mathbb{Z}/\ker \Phi = \mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im} \Phi$

$\mathbb{K}$ intègre, donc $\operatorname{Im} \Phi \subset \mathbb{K}$ sous-anneau intègre.

Rappel : $\mathbb{Z}/n\mathbb{Z}$ intègre SSI $n > 1$ est premier.

Donc la caractéristique n de $\mathbb{K}$ est un nombre premier
$\mathbb{K}$ contient un sous-champ $\cong \mathbb{Z}_n$. ($\mathbb{K}$ est une extension de $\mathbb{Z}_n$.)

Vers les champs finis

Conclusion

Tout champ fini $\mathbb{K}$ contient un champ isomorphe à $\mathbb{Z}_p$,
p premier, appelé le sous-champ premier de $\mathbb{K}$.

Nous montrerons l'unicité du sous-champ premier, i.e.,
$\mathbb{Z}_p$ est l'unique champ de la forme $\mathbb{Z}_m$ inclus dans $\mathbb{K}$.

Vers les champs finis

Binôme de Newton "stupide"

Soit $\mathbb{K}$ est un champ de caractéristique p (p premier).

$$\forall a, b \in \mathbb{K}, \forall n \geq 1, \quad (a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Par récurrence sur n. Si $n = 1$.
Binôme de Newton "classique" (applicable dans tout champ)

$$(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{p-k}.$$

pour $0 < k < p$, $p! = k!\,(p-k)!\,C_p^k$, p ne divise pas $k!\,(p-k)!$.
C_p^k est un multiple de la caractéristique p donc $C_p^k = 0$ dans $\mathbb{K}$.

Vers les champs finis

OK pour $n-1$, OK pour n ?

$$(a+b)^{p^n} = ((a+b)^{p^{n-1}})^p = (a^{p^{n-1}} + b^{p^{n-1}})^p = a^{p^n} + b^{p^n}.$$

Pour l'avant-dernière égalité, on a utilisé l'hypothèse de récurrence et pour la dernière, le cas $n = 1$.

Vers les champs finis

Peut-on avoir un champ avec 15 éléments ?

Proposition

Soit $\mathbb{K}$ un champ fini de caractéristique $p > 1$.
Il existe $n > 0$ tel que $\mathbb{K}$ contienne exactement p^n éléments.

$\mathbb{K}$ contient un sous-champ isomorphe à $\mathbb{Z}_p$.

Considérer $\mathbb{K}$ comme un $\mathbb{Z}_p$-vectoriel et si $[\mathbb{K} : \mathbb{Z}_p] = n$,

alors $\#\mathbb{K} = p^n$.

Rappel

Si $\mathbb{K}$ est un champ fini contenant t éléments et si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré fini d, alors $\mathbb{L}$ contient t^d éléments.

Vers les champs finis

Peut-on avoir un champ avec 15 éléments ?

Proposition

Soit $\mathbb{K}$ un champ fini de caractéristique $p > 1$.
Il existe $n > 0$ tel que $\mathbb{K}$ contienne exactement p^n éléments.

$\mathbb{K}$ contient un sous-champ isomorphe à $\mathbb{Z}_p$.

Considérer $\mathbb{K}$ comme un $\mathbb{Z}_p$-vectoriel et si $[\mathbb{K} : \mathbb{Z}_p] = n$,

alors $\#\mathbb{K} = p^n$.

Rappel

Si $\mathbb{K}$ est un champ fini contenant t éléments et si $\mathbb{L}$ est une extension de $\mathbb{K}$ de degré fini d, alors $\mathbb{L}$ contient t^d éléments.

Vers les champs finis

Corollaire

Soit $\mathbb{K}$ un champ fini, le seul champ de la forme $\mathbb{Z}_q$, $q \geq 2$, inclus dans $\mathbb{K}$ est son sous-champ premier.

Si $\mathrm{Car}\,\mathbb{K} = p$, i.e., si $\mathbb{K}$ a $\mathbb{Z}_p$ comme sous-champ premier.

$\mathbb{K}$ contient p^n éléments (vu résultat préc.)

Supposons que $\mathbb{Z}_q$ est un sous-champ de $\mathbb{K}$.
q divise p^n (ordre d'un sous-groupe divise ordre du groupe).
$\mathbb{Z}_q$ est un champ, q premier. Par conséquent, $q = p$.

VERS LES CHAMPS FINIS

L. Euler

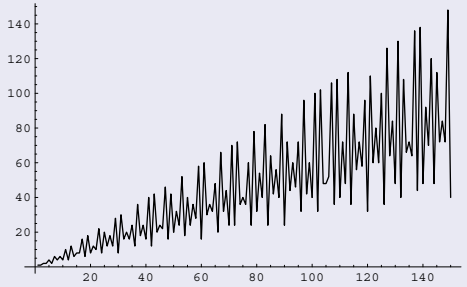
VERS LES CHAMPS FINIS

DÉFINITION

Fonction indicatrice d'Euleur ou fonction totient

$$\varphi(n) = \begin{cases} 1, & \text{si } n = 1 \\ \#\{x \mid 1 \leq x \leq n,\ \text{pcgd}(x,n) = 1\}, & \text{si } n > 1. \end{cases}$$

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4



VERS LES CHAMPS FINIS

REMARQUE

Le groupe multiplicatif $\mathbb{Z}_n^*$ est d'ordre $\varphi(n)$.

LEMME

φ est multiplicative, i.e.,
si m et n sont des entiers premiers entre eux, alors

$$\varphi(mn) = \varphi(m)\varphi(n).$$

m et n sont premiers entre eux, l'anneau $\mathbb{Z}_{mn}$ est $\tilde{=}$ à $\mathbb{Z}_m \times \mathbb{Z}_n$.

D'où isomorphisme de groupes entre $\mathbb{Z}_{mn}^*$ et $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

VERS LES CHAMPS FINIS

Soit $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ l'isomorphisme.

$\forall z \in \mathbb{Z}_{mn}$, il correspond un unique $\varphi(z) = (z_1, z_2)$ et réct.

Si z est inversible et a z' pour inverse, alors

$$\varphi(z.z') = \varphi(z).\varphi(z') = \varphi(1) = (1,1).$$

$$(z_1, z_2).(z_1', z_2') = (1,1) = (z_1 z_1', z_2 z_2')$$

donc z_1 (resp. z_2) est un élément inversible de $\mathbb{Z}_m$ (resp. $\mathbb{Z}_n$).

réciproque : idem

Vers les champs finis

Corollaire

Si $n = p_1^{k_1} \cdots p_r^{k_r}$, alors

$$\varphi(n) = \prod_{j=1}^{r} (p_j - 1)\, p_j^{k_j - 1}.$$

Thèse' : $\varphi(p^k) = (p-1)\,p^{k-1}$, p premier.

les nombres entiers dans $[1, p^k]$ non premiers avec p^k sont les multiples de p :

$$p, 2p, 3p, \ldots, (p^{k-1} - 1)\,p, p^{k-1}\,p$$

il y en a p^{k-1} et $p^k - p^{k-1} = (p-1)\,p^{k-1}$.

Vers les champs finis

Petit théorème de Fermat / Euler

Si $\mathrm{pgcd}(a, m) = 1$, alors $a^{\varphi(m)} \equiv 1 \mod m$.

$\mathrm{pgcd}(a, m) = 1$ donc $a \in \mathbb{Z}_m^*$.
L'ordre d'un élément divise l'ordre du groupe.

Remarque : $a < m$? $a > m$?

Si $a > m$, division euclidienne $a = q.m + a'$ avec $a' < m$.
Si $\mathrm{pgcd}(a, m) = 1$, alors $\mathrm{pgcd}(a', m) = 1$ et $a \equiv a' \mod m$.

Autre formulation, cas particulier

Soient p un nombre premier et $n < p$ un entier. On a

$$n^p \equiv n \mod p.$$

Vers les champs finis

Petit théorème de Fermat / Euler

Si $\mathrm{pgcd}(a, m) = 1$, alors $a^{\varphi(m)} \equiv 1 \mod m$.

$\mathrm{pgcd}(a, m) = 1$ donc $a \in \mathbb{Z}_m^*$.
L'ordre d'un élément divise l'ordre du groupe.

Remarque : $a < m$? $a > m$?

Si $a > m$, division euclidienne $a = q.m + a'$ avec $a' < m$.
Si $\mathrm{pgcd}(a, m) = 1$, alors $\mathrm{pgcd}(a', m) = 1$ et $a \equiv a' \mod m$.

Autre formulation, cas particulier

Soient p un nombre premier et $n < p$ un entier. On a

$$n^p \equiv n \mod p.$$

Vers les champs finis

Théorème de Wilson

p un nombre premier, $(p-1)! \equiv -1 \mod p$.

$p \geq 3$. Classer les éléments de $\mathbb{Z}_p^*$ selon qu'ils sont ou non égaux à leur inverse.

Si $x = x^{-1}$, alors $x^2 = 1$ et x racine de $X^2 - 1 \in \mathbb{Z}_p[X]$ qui n'a que 2 racines -1 et 1.
1 et -1 sont les seuls éléments de $\mathbb{Z}_p^*$ égaux à leur inverse.

Les $p-3$ autres éléments de $\mathbb{Z}_p^*$ se groupent par paires d'éléments distincts (x_i, y_i), $1 \leq i \leq (p-3)/2$, $x_i y_i = 1$.

$(p-1)!$ est le produit de tous les éléments de $\mathbb{Z}_p^*$,

$$(p-1)! = 1.(-1). \prod_{i=1}^{(p-3)/2} x_i y_i = -1.$$

Vers les champs finis

Remarque, mieux que thm. de Wilson

$m > 1$ est premier **SSI** $(m-1)! \equiv -1 \mod m$.

Si m n'est pas premier, $m = a.b$ avec $1 < a < m$.

a divise $(m-1)!$.
a ne divise pas $(m-1)!+1$.
m ne divise pas $(m-1)!+1$ car sinon...

Test de primalité

m est-il premier ? calculer $(m-1)! \mod m$...

Peu effectif !

Structure des champs finis

Définition

Dans $\mathbb{F}_q$, générateur (multiplicatif) de $\mathbb{F}_q$: tout élément g d'ordre $q-1$ pour le groupe multiplicatif $\mathbb{F}_q^*$ (ou élément primitif)
$\mathbb{F}_q^* = \{g^n \mid n = 1, \ldots, q-1\}$.

Exemple

Dans $\mathbb{Z}_5$, 2 est un générateur :

i	1	2	3	4
2^i	2	4	3	1

Définition

Si g générateur de $\mathbb{F}_q$, logarithme discret en base g :
$\mathrm{dlog}_g \alpha = n$ si $g^n = \alpha$ avec $n < q$, $\alpha \neq 0$.

Structure des champs finis

$\mathbb{F}_q^*$ est un groupe cyclique.

Théorème

- Tout champ fini $\mathbb{F}_q$ possède un générateur.
- Si g est un générateur de $\mathbb{F}_q$, alors g^j en est un aussi SSI $\mathrm{pgcd}(j, q-1) = 1$.
- Le nombre de générateurs de $\mathbb{F}_q$ est $\varphi(q-1)$.

Structure des champs finis

Lemme

Pour tout entier $N \geq 2$, on a $\sum_{d|N} \varphi(d) = N$.

Partition de $E = \{1, 2, \ldots, N\}$ en ensembles disjoints E_d.

Pour chaque diviseur d de N, $E_d := \{k \in E \mid \mathrm{pgcd}(k, N) = d\}$.

$\#E_d = ?$
Soit $k \in E_d$. Puisque $\mathrm{pgcd}(k, N) = d$, il existe k' et N' t.q.

$$k = k'd, \ N = N'd \ \text{ et } \mathrm{pgcd}(k', N') = 1.$$

$1 \leq k \leq N$ donc $1 \leq k' \leq N'$. Il y a $\varphi(N')$ tels nombres k'.

A chaque k' correspond exactement un entier k de E_d.

Structure des champs finis

On en tire donc

$$\#E_d = \varphi(N') = \varphi(\frac{N}{d}).$$

Si $d_1, \ldots, d_r$ sont tous les diviseurs de N, on a

$$N = \#E = \sum_{i=1}^{r} \#E_{d_i} = \sum_{i=1}^{r} \varphi(\frac{N}{d_i}).$$

Pour conclure, il suffit de remarquer que

$$\{N/d_i \mid i = 1, \ldots, r\} = \{d_1, \ldots, d_r\}.$$

En effet, chaque N/d_i est lui-même un diviseur de N. Par conséquent, lorsqu'on parcourt l'ensemble des N/d_i possibles, on parcourt en fait l'ensemble de tous les diviseurs de N.

Structure des champs finis

Illustration

$18 = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)+\varphi(9)+\varphi(18) = 1+1+2+2+6+6.$

De plus,

$18 = \varphi(18/1)+\varphi(18/2)+\varphi(18/3)+\varphi(18/6)+\varphi(18/9)+\varphi(18/18)$

et

$$E_1 = \{1,5,7,11,13,17\}, \quad E_2 = \{2,4,8,10,14,16\},$$

$$E_3 = \{3,15\}, \quad E_6 = \{6,12\}, \quad E_9 = \{9\} \text{ et } E_{18} = \{18\}.$$

Structure des champs finis

Preuve du théorème...

Partie 1. Supposons qu'il existe a : élément d'ordre d de $\mathbb{F}_q^*$.

L'ordre d'un élément divise l'ordre du groupe : d divise $q-1$.
Par définition, d est le plus petit entier tel que $a^d = 1$.

Ainsi, $a, a^2, \ldots, a^d$ sont des éléments distincts.

Structure des champs finis

Partie 2. Les éléments d'ordre d de $\mathbb{F}_q^*$ sont exactement les a^j tels que $\text{pgcd}(j,d) = 1$.

$a, a^2, \ldots, a^d$ sont tous racines de $X^d - 1$.
Un polynôme de degré d possède au plus d racines.
$\Rightarrow \{a, a^2, \ldots, a^d\}$ = l'ensemble des racines de $X^d - 1$.

- Un élément d'ordre d de $\mathbb{F}_q^*$ est racine de $X^d - 1$.
Il est donc de la forme a^j.

- Tout a^j n'est pas nécessairement d'ordre d.
Si $\text{pgcd}(j,d) = d' > 1$, alors $(a^j)^{d/d'} = (a^d)^{j/d'} = 1$
ordre de a^j divise $d/d' < d$, a^j n'est pas d'ordre d.

Si $\text{pgcd}(j,d) = 1$, $\exists\, u, v : 1 = ju - dv$, $a = a^{1+dv} = (a^j)^u$

a et a^j sont puissances l'un de l'autre donc de même ordre d.

Structure des champs finis

Rappel

Si $x^m = y$ et $y^n = x$, alors x et y sont de même ordre.

En effet, si x (resp. y) est d'ordre k (resp. ℓ), alors $y^k = (x^m)^k = (x^k)^m = 1$ et donc $\ell \leq k$.

Par symétrie, $k \leq \ell$.

Si un élément d'ordre d existe dans $\mathbb{F}_q^*$, il y en a alors exactement $\varphi(d)$.

$\forall d$ divisant $q-1$, deux possibilités :

- aucun élément de $\mathbb{F}_q^*$ n'est d'ordre d
- il y a exactement $\varphi(d)$ éléments d'ordre d.

Structure des champs finis

Partie 3. Argument de comptage.

Lemme précédent avec $N = q-1$.

Dans $\mathbb{F}_q^*$, l'ordre de tout élément divise $q-1$.
Il faut nécessairement $\varphi(d)$ éléments d'ordre d, $\forall d | (q-1)$.

En particulier, $\mathbb{F}_q^*$ contient $\varphi(q-1)$ éléments d'ordre $q-1$. **QED**

Structure des champs finis

Illustration

$\mathbb{F}_9 = \mathbb{Z}_3[X]/\langle X^2+1 \rangle$

P	P^2	P^3	P^4	P^5	P^6	P^7	P^8
1							
2	1						
X	2	$2X$	1				
$2X$	2	X	1				
$X+1$	$2X$	$2X+1$	2	$2X+2$	X	$X+2$	1
$X+2$	X	$2X+2$	2	$2X+1$	$2X$	$X+1$	1
$2X+1$	X	$X+1$	2	$X+2$	$2X$	$2X+2$	1
$2X+2$	$2X$	$X+2$	2	$X+1$	X	$2X+1$	1

$\varphi(8) = 4$ (resp. $\varphi(4) = 2$, $\varphi(2) = 1$, $\varphi(1) = 1$) éléments d'ordre 8 (resp. 4, 2, 1).

Unicité d'un champ à p^f éléments

Théorème

Soit $\mathbb{F}_q$ un champ à $q = p^f$ éléments.
Tout élément de $\mathbb{F}_q$ satisfait l'équation $X^q - X = 0$ et $\mathbb{F}_q$ est précisément l'ensemble des racines de cette équation.
Autrement dit, pour tout sous-champ $\mathbb{K}$ de $\mathbb{F}_q$, $\mathbb{F}_q$ est le corps de rupture du polynôme $X^q - X$ sur $\mathbb{K}$.

Réciproquement, pour tout $q = p^f$, puissance d'un nombre premier p, le corps de rupture du polynôme $X^q - X$ sur $\mathbb{Z}_p$ est un champ à q éléments.

$\rightarrow$ "Unicité de F_q, vu unicité du corps de rupture".

Unicité d'un champ à p^f éléments

Partie 1. Soit $\mathbb{F}_q$ champ fini de car. p.

L'ordre de tout élément $\neq 0$ divise $q-1$,
tout élément $\neq 0$ satisfait l'équation $X^{q-1}=1$ donc $X^q=X$.

L'élément nul satisfait aussi $X^q=X$.

Tout élément de $\mathbb{F}_q$ est racine de X^q-X.

Pour tout $\mathbb{K}$ sous-champ de $\mathbb{F}_q$, considérer $X^q-X \in \mathbb{K}[X]$.

Puisque ce polynôme a au plus q racines, ses racines décrivent donc exactement $\mathbb{F}_q$, i.e.,
$\mathbb{F}_q$ est le corps de rupture de X^q-X sur $\mathbb{K}$.

Unicité d'un champ à p^f éléments

Partie 2. $q=p^f$, $\mathbb{F}$: corps de rupture de $P=X^q-X$ sur $\mathbb{Z}_p$.

$D_X(X^q-X)=qX^{q-1}-1=-1$ (car $q=p^f$ et carac. p).
X^q-X n'a pas de racine mutliple (ni sur $\mathbb{Z}_p$, ni sur $\mathbb{F}$).

$\mathbb{F}$ contient au moins les q racines distinctes de P ($\#\mathbb{F} \geq q$).

Il suffit de montrer que l'ensemble de ces racines est un champ (en effet, le corps de rupture est le plus petit champ contenant ces racines).

Soient a et b, deux racines, i.e., $a^q=a$ et $b^q=b$.
Produit des racines est une racine car $(ab)^q=ab$.
Pour la somme ($\mathbb{F}$ est une extension de $\mathbb{Z}_p$ donc de car. p), on a $(a+b)^q=a^q+b^q=a+b$.
L'inverse, $a^q=a \Rightarrow a^{-q-1}.a^q=a^{-q-1}.a$ donc $a^{-1}=(a^{-1})^q$.
L'opposé $(a+(-a))^q=0=a^q+(-a)^q$ donc, $(-a)^q=-(a^q)$.

Unicité d'un champ à p^f éléments

Remarque

Soit $\mathbb{K}$ un sous-champ de $\mathbb{F}_q$. Puisque $\mathbb{F}_q$ est le corps de rupture de X^q-X sur $\mathbb{K}$, on a

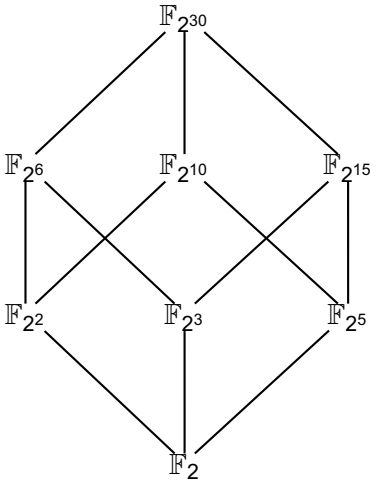
$$X^q-X=\prod_{\alpha\in\mathbb{F}_q}(X-\alpha).$$

Remarque

Tout élément de $\mathbb{F}_q$ est algébrique sur $\mathbb{F}_p$ (et même sur tout sous-champ $\mathbb{K}$ de $\mathbb{F}_q$).

Tout élément de $\mathbb{F}_q$ est racine du polynôme $X^q-X \in \mathbb{F}_p[X]$ (on peut considérer que $X^q-X \in \mathbb{K}[X]$).

Sous-champs de $\mathbb{F}_q$



Sous-champs de $\mathbb{F}_q$

Lemme

Soient $m > n$. Le pgcd de $X^{p^m} - X$ et de $X^{p^n} - X$ est $X^{p^h} - X$ où $h = \mathrm{pgcd}(m, n)$. En particulier, si d divise f, alors $X^{p^d} - X$ divise $X^{p^f} - X$.

Division euclidienne, $m = a.n + r$ avec $0 \leq r < n$.

Alors, on obtient

$$p^m - 1 = (p^n - 1)\,(\underbrace{p^{(a-1)n} + p^{(a-2)n} + \cdots + p^n + 1}_{:=\alpha})\,p^r + p^r - 1$$

$$X^{p^m-1} - 1 = X^{(p^n-1)\,\alpha\,p^r + p^r - 1} - 1 = X^{p^r-1}(X^{(p^n-1)\,\alpha\,p^r} - 1) + X^{p^r-1} - 1.$$

$$X^{(p^n-1)\,\alpha\,p^r} - 1 = (X^{p^n-1} - 1)(\underbrace{(X^{p^n-1})^{\alpha\,p^r-1} + (X^{p^n-1})^{\alpha\,p^r-2} + \cdots + 1}_{:=Q}).$$

$$X^{p^m} - X = X^{p^r-1}\,(X^{p^n} - X)\,Q + X^{p^r} - X.$$

le reste de la division de $X^{p^m} - X$ par $X^{p^n} - X$= $X^{p^r} - X$.

Sous-champs de $\mathbb{F}_q$

On conclut en utilisant l'algorithme d'Euclide et en procédant par divisions euclidiennes successives.

Le pgcd de $X^{p^m} - X$ et de $X^{p^n} - X$ est égal à celui de $X^{p^n} - X$ et de $X^{p^r} - X$, et ainsi de suite...

Sous-champs de $\mathbb{F}_q$

Théorème

Les sous-champs de $\mathbb{F}_q = \mathbb{F}_{p^f}$ sont exactement les $\mathbb{F}_{p^d}$ pour d divisant f. Plus précisément, si $\mathbb{K}$ est un sous-champ de $\mathbb{F}_q$, alors il contient p^d éléments où d divise f.
Réciproquement, si d divise f, alors $\mathbb{F}_q$ contient exactement un sous-champ contenant p^d éléments.

En particulier, si on étend $\mathbb{F}_p$ par un élément de $\mathbb{F}_{p^f}$, alors on obtient un de ces sous-champs $\mathbb{F}_{p^d}$.

$\Rightarrow$: Soit $\mathbb{K}$ un sous-champ de $\mathbb{F}_q$ contenant t éléments.

Si $[\mathbb{F}_q : \mathbb{K}] = s$, alors $\#\mathbb{F}_q = t^s$ et $p^f = t^s$.
p est premier donc $\exists\ d$ tel que $t = p^d$ et $ds = f$

Sous-champs de $\mathbb{F}_q$

$\Leftarrow$: Soit d un diviseur de f. Au vu du lemme précédent, $X^{p^d} - X$ divise $X^{p^f} - X = X^q - X$ (nous allons considérer ces deux polynômes comme polynômes sur $\mathbb{Z}_p$).

Toute racine de $X^{p^d} - X$ est racine de $X^q - X$ et appartient donc à $\mathbb{F}_q$ (cf. thm..., $\mathbb{F}_q$ corps de rupture...).

Donc $\mathbb{F}_q$ contient le corps de rupture de $X^{p^d} - X$ sur $\mathbb{Z}_p$.

Vu le thm..., ce corps de rupture est un champ à p^d éléments.

càd. $\mathbb{F}_q$ contient un sous-champ à p^d éléments.

Supposons que $\mathbb{F}_q$ contienne au moins 2 tels sous-champs $\neq$.

Ensemble, ils contiendraient plus de p^d racines de $X^{p^d} - X$, impossible !

Ceci prouve l'unicité du sous-champ d'ordre p^d.

Sous-champs de $\mathbb{F}_q$

Pour finir la preuve, il reste

En particulier…

Si on étend $\mathbb{F}_p$ par un élément de $\mathbb{F}_{p^f}$, alors on obtient un de ces sous-champs $\mathbb{F}_{p^d}$.

$\mathbb{F}_p(\alpha)$ est un sous-champ de $\mathbb{F}_q$. Il est donc de la forme $\mathbb{F}_{p^d}$ pour un certain d divisant f.

Sous-champs de $\mathbb{F}_q$

Exemple

$\mathbb{F}_{2^8} = \mathbb{F}_{256}$, diviseurs de 8 : $1, 2, 4, 8$, les sous-champs propres de $\mathbb{F}_{2^8}$ sont $\mathbb{F}_2$, $\mathbb{F}_{2^2}$ et $\mathbb{F}_{2^4}$. On obtient un treillis “linéaire”

Sous-champs de $\mathbb{F}_q$

Pour chaque sous-champ : ordre et nombre d’élts ?

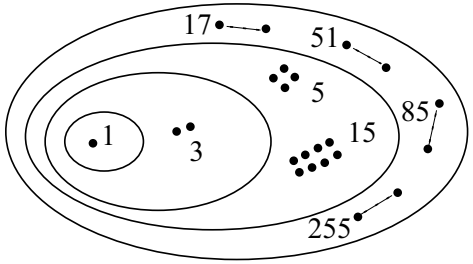
Rappel

$\forall d$ diviseur de $q-1$, dans $\mathbb{F}_q^*$ exactement $\varphi(d)$ éléments d’ordre d.

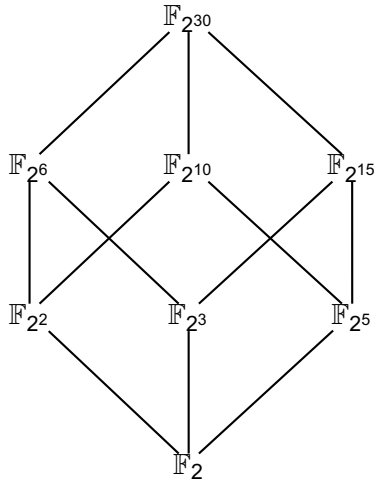
Dans ce tableau, il faut comprendre que tous les éléments repris dans les k premières lignes appartiennent aussi aux sous-champs apparaissant “plus bas” (à cause de l’emboîtement).

	ord	#
$\mathbb{F}_2^*$	1	1
$\mathbb{F}_4^*$	3	2
$\mathbb{F}_{16}^*$	5	4
	15	8
$\mathbb{F}_{256}^*$	17	16
	51	32
	85	64
	255	128

Sous-champs de $\mathbb{F}_q$



Sous-champs de $\mathbb{F}_q$



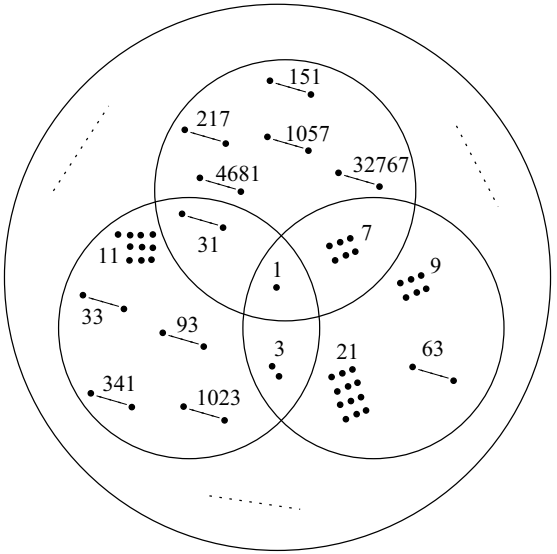
Sous-champs de $\mathbb{F}_q$

	ord	#	déjà pris en compte
$\mathbb{F}_2^*$	1	1	
$\mathbb{F}_{2^2}^*$	3	2	1
$\mathbb{F}_{2^3}^*$	7	6	1
$\mathbb{F}_{2^5}^*$	31	30	1
$\mathbb{F}_{2^6}^*$	9	6	1, 3, 7
	21	12	
	63	36	
$\mathbb{F}_{2^{10}}^*$	11	10	1, 3, 31
	33	20	
	93	60	
	341	300	
	1023	600	

Sous-champs de $\mathbb{F}_q$

	ord	#	déjà pris en compte
$\mathbb{F}_{2^{15}}^*$			1, 7, 31
	151	150	
	217	180	
	1057	900	
	4681	4500	
	32767	27000	
$\mathbb{F}_{2^{30}}^*$			1, 3, 7, 9, 11, 21, 31, 33 63, 93, 151, 217, 341, 1023, 1057, 4681, 32767
	77	60	
	99	60	
	231	120	
	⋮	⋮	
	1073741823	534600000	

Sous-champs de $\mathbb{F}_q$



Construction de champs finis

- p premier, $\mathbb{Z}_p$ est un champ (le champ $\mathbb{F}_p$)
  on connaît sa structure et l'arithmétique modulo p.
- $q = p^f$, $\mathbb{F}_q$: quotient de l'anneau $\mathbb{F}_p[X]$ par un polynôme irréductible de degré f.
  Variante : considérer une extension de $\mathbb{F}_p$ par une racine d'un polynôme irréductible de degré f sur $\mathbb{F}_p$.

Question : existence de polynômes irréductibles sur $\mathbb{F}_p$ de degré f ?

Construction de champs finis

Théorème

$\forall q = p^f$, le polynôme $X^q - X$ est le produit dans $\mathbb{F}_p[X]$ de tous les polynômes minimums (distincts) des éléments de $\mathbb{F}_q$.

$\mathbb{F}_q$ est précisément l'ensemble des racines de $X^q - X$ et ce polynôme ne possède pas de racine multiple (cf. thm...).

Si $\beta \in \mathbb{F}_q$, il est algébrique sur $\mathbb{F}_p$ (car $X^q - X$ peut être vu comme un polynôme de $\mathbb{F}_p[X]$ qui est annulé par β) et possède M_β comme polynôme minimum sur $\mathbb{F}_p$, alors M_β divise $X^q - X$.

Si $\alpha, \beta \in \mathbb{F}_q$ (resp. M_α, M_β comme polynôme minimum sur $\mathbb{F}_p$), alors

- soit $M_\alpha = M_\beta$ (autrement dit, α et β sont conjugués)
- soit $M_\alpha \neq M_\beta$ et ces polynômes n'ont aucune racine commune (car sinon, ils auraient une racine commune γ, conjugué de α et β ; on pourrait alors conclure que $M_\alpha = M_\gamma = M_\beta$).

Construction de champs finis

$\mathbb{F}_q$ peut être partitionné en classes telles que $\alpha, \beta \in \mathbb{F}_q$ appartiennent à une même classe SSI $M_\alpha = M_\beta$ (relation d'équivalence).

Si $\mathbb{F}_q$ est partitionné en t classes et en choisissant un représentant $\alpha_1, \ldots, \alpha_t$ dans chaque classe, on trouve

$$X^q - X = M_{\alpha_1} \cdots M_{\alpha_t}.$$

De proche en proche. On a $X^q - X = M_{\alpha_1} Q$.
Puisque les racines de $X^q - X$ sont simples, M_{α_1} et Q n'ont pas de racine commune et les racines de $X^q - X$ non conjugées à α_1 sont exactement les racines de Q. On continue de proche en proche jusqu'à avoir épuisé $\mathbb{F}_q$.

Construction de champs finis

Théorème

$q = p^f$, $X^q - X$ se factorise dans $\mathbb{F}_p[X]$ en le produit de tous les polynômes moniques irréductibles (distincts) dont le degré divise f.

$X^q - X$ est le produit dans $\mathbb{F}_p[X]$ de tous les polynômes minimums (distincts) des éléments de $\mathbb{F}_q$.

Soit P un tel polynôme de deg d, polynôme minimum de $\alpha \in \mathbb{F}_q$.

P est irréductible, $\mathbb{F}_p[X]/\langle P \rangle$ est un champ à p^d éléments.

Ce champ est isomorphe à $\mathbb{F}_p(\alpha)$. Il s'agit donc d'un sous-champ de $\mathbb{F}_q$.

Par le thm de structure des sous-champs de $\mathbb{F}_q$: d divise f.

Construction de champs finis

Il nous reste à montrer que tout polynôme P monique irréductible sur $\mathbb{F}_p$ dont le degré d divise f est le polynôme minimum sur $\mathbb{F}_p$ d'un élément de $\mathbb{F}_q$.

$\mathbb{L} = \mathbb{F}_p[X]/\langle P \rangle$ champ contenant p^d éléments.

Par le thm de structure des sous-champs de $\mathbb{F}_q$, $\mathbb{L}$ est (isomorphe à) un sous-champ de $\mathbb{F}_q$.

De plus, par construction, $\mathbb{L}$ (et donc $\mathbb{F}_q$) contient une racine β de P. Autrement dit, P est un polynôme monique irréductible sur $\mathbb{F}_p$ ayant $\beta \in \mathbb{F}_q$ comme racine : P est le polynôme minimum de β sur $\mathbb{F}_p$.

Construction de champs finis

Corollaire

f premier, il y a exactement $\frac{p^f - p}{f}$ polynômes moniques irréductibles de degré f dans $\mathbb{F}_p[X]$.

Remarque

Petit théorème de Fermat, $p^f \equiv p \mod f$.

$N_p(f) = \#$ polynômes moniques irréductibles de deg. $f \in \mathbb{F}_p[X]$.

Par le théorème précédent, les seuls diviseurs de f étant 1 et f, le polynôme $X^{p^f} - X$ se factorise en un produit

- des $N_p(f) = k$ polynômes $P_1, \ldots, P_k$ moniques irréductibles sur $\mathbb{F}_p$ de degré f et
- des p polynômes de degré un : $X - \alpha_i$, pour $\alpha_i \in \mathbb{F}_p$, $i = 1, \ldots, p$.

Construction de champs finis

$$X^{p^f} - X = \underbrace{P_1(X) \cdots P_k(X)}_{N_p(f) \text{ polynômes de degré } f} \underbrace{(X - \alpha_1) \cdots (X - \alpha_p)}_{p \text{ polynômes de degré } 1}$$

et en s'intéressant au degré des deux membres, on obtient

$$p^f = f.N_p(f) + p$$

Construction de champs finis

Remarque

Si f n'est pas premier.
$N_p(d) = \#$ polynômes moniques irréductibles de deg d sur $\mathbb{F}_p$.

Au vu du thm...

$$p^f = \sum_{d|f} d.N_p(d) = f.N_p(f) + \sum_{\substack{d|f \\ d<f}} d.N_p(d)$$

$$N_p(f) = \left(p^f - \sum_{\substack{d|f \\ d<f}} d.N_p(d) \right) / f.$$

calculer de proche en proche $N_p(f)\ldots$ "rassurant !"

Construction de champs finis

$$N_p(f) = \left(p^f - \sum_{\substack{d|f \\ d<f}} d.N_p(d) \right) / f.$$

```
In[3]:= Divisors[18]
Out[3]= {1, 2, 3, 6, 9, 18}

In[4]:= Drop[Divisors[18], -1]
Out[4]= {1, 2, 3, 6, 9}

In[5]:= Map[#^2 &, Drop[Divisors[18], -1]]
Out[5]= {1, 4, 9, 36, 81}

In[1]:= n[p_, f_] := (p^f - Map[n[p, #] &, Drop[Divisors[f], -1]].Drop[Divisors[f], -1]) / f

In[7]:= Table[n[Prime[i], j], {i, 1, 3}, {j, 1, 4}]
Out[7]= {{2, 1, 2, 3}, {3, 3, 8, 18}, {5, 10, 40, 150}}
```

Construction de champs finis

f	1	2	3	4	5	6	7
p	2	1	2	3	6	9	18
	3	3	8	18	48	116	312
	5	10	40	150	624	2580	11160
	7	21	112	588	3360	19544	117648
	11	55	440	3630	32208	295020	2783880
	13	78	728	7098	74256	804076	8964072
	17	136	1632	20808	283968	4022064	58619808
	19	171	2280	32490	495216	7839780	127695960
	23	253	4048	69828	1287264	24670536	486403632
	29	406	8120	176610	4102224	99133020	2464268040

Construction de champs finis

Remarque

On peut montrer que

$$\frac{N_p(f)}{p^f} \sim \frac{1}{f}$$

Remarque

En pratique, pour générer un polynôme monique irréductible sur $\mathbb{F}_p$ de degré f, on choisit de manière aléatoire un polynôme monique puis on teste si le polynôme obtenu est ou non irréductible.

Construction de champs finis

Méthode naïve. . . comparer avec tous les polynômes irréductibles de deg <

```
In[24]:= p = 2;

         (* genere tous les polynomes de degre d sur Z_p *)

In[25]:= genere[d_] :=
           Table[IntegerDigits[i, p].Reverse[Table[x^i, {i, 0, d}]], {i, p^d, p^(d + 1) - 1}]

         (* initialise la liste des poly. irreductibles, ceux de deg = 1 *)

In[29]:= liste = genere[1]
Out[29]= {x, 1 + x}

         (* test si un poly est irreductible par rapport a la liste *)

In[30]:= irreductible[pol_] :=
           If[CoefficientList[Apply[Times, Map[PolynomialMod[pol, #, Modulus → p] &, liste]], x] ==
             {}, False, True]

In[31]:= Select[genere[2], irreductible[#] &]
Out[31]= {1 + x + x^2}
```

Construction de champs finis

```
(* generer tous les poly. irreductibles de deg <4 *)

In[33]:= liste = genere[1];
         For[i = 2, i < 4, liste = Flatten[Append[liste, Select[genere[i], irreductible[#] &]]];
          i++
         ]

In[35]:= liste

Out[35]= {x, 1 + x, 1 + x + x^2, 1 + x + x^3, 1 + x^2 + x^3}
```

Construction de champs finis

Proposition

Pour tout $n > 2$, le nombre de polynômes moniques irréductibles de degré n dans $\mathbb{F}_p[X]$ est minoré par

$$\frac{p^n - p\sqrt{p^n}}{n}.$$

Patience pour la preuve...

Définition

Soient $\mathbb{K} \subset \mathbb{L}$ deux champs. Un élément $\alpha \in \mathbb{L}$ est un générateur de $\mathbb{L}$ sur $\mathbb{K}$ si $\mathbb{L} = \mathbb{K}[\alpha]$

Construction de champs finis

Exemple

$\mathbb{F}_{16}$ comme $\mathbb{Z}_2[X]/\langle X^4 + X^3 + 1\rangle$,

X (i.e., $X + \langle X^4 + X^3 + 1\rangle$ est un "vrai" générateur mais que $X + 1$ n'en est pas un.

```
In[1]:= Union[Table[PolynomialMod[x^i, x^4 + x^3 + 1, Modulus -> 2], {i, 1, 15}]]

Out[1]= {1, x, x^2, x^3, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2, 1 + x^3,
         x + x^3, 1 + x + x^3, x^2 + x^3, 1 + x^2 + x^3, x + x^2 + x^3, 1 + x + x^2 + x^3}

In[2]:= Length[%]

Out[2]= 15

In[3]:= Union[Table[PolynomialMod[(x + 1)^i, x^4 + x^3 + 1, Modulus -> 2], {i, 1, 15}]]

Out[3]= {1, x^3, 1 + x, 1 + x^2, 1 + x + x^2 + x^3}
```

Construction de champs finis

Suite de l'exemple

$X + 1$ est un générateur de $\mathbb{F}_{16}$ sur $\mathbb{Z}_2$.

Il suffit de montrer que $X + \langle X^4 + X^3 + 1\rangle$ s'obtient comme un polynôme à coefficients dans $\mathbb{Z}_2$ de $X + 1 + \langle X^4 + X^3 + 1\rangle$

$$(X + 1)^5 + X + 1 = X \mod X^4 + X^3 + 1.$$

Tout élément de $\mathbb{Z}_2[X]/\langle X^4 + X^3 + 1\rangle$ s'obtient comme une expression polynomiale de $X + 1$.

Construction de champs finis

Proposition

Soient $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^{sn}}$ deux champs, $n > 2$. Le nombre de générateurs de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$ est $\geq p^{sn} - p^{s(1+\frac{n}{2})}$

α n'est PAS un générateur de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$
SSI $\alpha \in$ un sous-champ propre de $\mathbb{F}_{p^{sn}}$ qui contient $\mathbb{F}_{p^s}$.

Un tel sous-champ est de la forme $\mathbb{F}_{p^{sd}}$ où $d < n$ et $d|n$.

Le nombre de générateurs de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$ est $\geq$

$$p^{sn} - \sum_{\substack{d|n \\ d<n}} p^{sd} \geq p^{sn} - \sum_{r=1}^{\lfloor n/2 \rfloor} p^{sr} = p^{sn} - p^s \frac{p^{s\lfloor n/2 \rfloor} - 1}{p^s - 1} \geq p^{sn} - p^{s(1+n/2)}$$

car on remarque que $\frac{p^{s\lfloor n/2 \rfloor}-1}{p^s-1} \leq p^{sn/2}$.

Construction de champs finis

Lemme

Soient $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^{sn}}$ deux champs, $n \geq 2$. L'élément $\alpha \in \mathbb{F}_{p^{sn}}$ est un générateur de $\mathbb{F}_{p^{sn}}$ sur $\mathbb{F}_{p^s}$ SSI son polynôme minimum sur $\mathbb{F}_{p^s}$ est de degré n.

M_α polynôme minimum de α sur $\mathbb{F}_{p^s}$.
(on sait que α est algébrique sur $\mathbb{F}_{p^s}$ et donc $\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^s}(\alpha)$)

$\Leftarrow$: Si $\deg M_\alpha = n$, alors $\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^s}(\alpha) \cong \mathbb{F}_{p^s}[X]/\langle M_\alpha \rangle$ qui possède p^{sn} éléments, i.e.,

$$\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^{sn}}$$

$\Rightarrow$: Si $\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^{sn}}$, alors $\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^s}(\alpha) \simeq \mathbb{F}_{p^s}[X]/\langle M_\alpha \rangle$ possède p^{sn} éléments et on en déduit que $\deg M_\alpha = n$.

Construction de champs finis

Proposition

Pour tout $n > 2$, le nombre de polynômes moniques irréductibles de degré n dans $\mathbb{F}_p[X]$ est $\geq \frac{p^n - p\sqrt{p^n}}{n}$.

$\mathbb{F}_{p^n}$ contient $\mathbb{F}_p$ comme sous-champ.
Le nombre de générateurs de $\mathbb{F}_{p^n}$ sur $\mathbb{F}_p$ est $\geq p^n - p\sqrt{p^n}$.

Soit α un tel générateur. Par le lemme précédent, son polynôme minimum sur $\mathbb{F}_p$ (qui est monique et irréductible) est de degré n.

Ce polynôme possède au plus n racines. Autrement dit, il est le polynôme minimum d'au plus n des générateurs envisagés.

Donc le nombre de polynômes moniques irréductibles de $\mathbb{F}_p[X]$ est $\geq (p^n - p\sqrt{p^n})/n$.

Construction de champs finis

minoration de $N_p(n)$ donné par la proposition précédente

p \ n	3	4	5	6	7
2	1	3	5	9	17
3	7	18	47	120	311
5	38	153	622	2602	11158
7	110	596	3358	19605	117646
11	437	3654	32205	295255	2783877
13	724	7133	74252	804462	8964068
17	1627	20871	283963	4022921	58619804
19	2275	32570	495211	7840972	127695955
23	4042	69948	1287258	24672638	486403626
29	8112	176805	4102216	99137208	2464268033

Représentation en base entière

base $b \geq 2$

$$n = \sum_{i=0}^{\ell-1} \sigma_i \, b^i, \quad \text{avec } \sigma_i \in \{0, \ldots, b-1\} \text{ et } \sigma_{\ell-1} \neq 0.$$

$\rho_b(n) = \sigma_{\ell-1} \cdots \sigma_0$: représentation en base b de n.
$\sigma_{\ell-1}$: chiffre de poids fort ou chiffre le plus significatif
σ_0 : chiffre de poids faible ou le chiffre le moins significatif.

$\forall n \geq 1, \exists \ell \geq 0 : b^{\ell-1} \leq n < b^\ell$, $\rho_b(n)$ est un mot de longueur ℓ.
$L_b(n) = \ell$: longueur de la représentation en base b de n

$$L_b(n) = \lfloor \log_b(n) \rfloor + 1 = \left\lfloor \frac{\ln n}{\ln b} \right\rfloor + 1.$$

Exponentiation modulaire

$$x^e \mod m \quad \text{avec} \quad e = \sum_{i=0}^{k} e_i \, 2^i.$$

$$x^e = x^{\sum_{i=0}^{k} e_i \, 2^i} = \prod_{i=0}^{k} (x^{2^i})^{e_i} = \prod_{\substack{0 \leq i \leq k \\ e_i = 1}} x^{2^i}.$$

$$x^{2^{i+1}} = (x^{2^i})^2$$

- calculer les $x^{2^i} \mod m$ au moyen de $L_b(e) - 1$ élévations successives au carré (mod m)
- calculer $L_b(e) - 1$ produits (mod m).

complexité de l'algorithme : logarithmique en e et non pas linéaire comme l'aurait été un algorithme naïf !

Exponentiation modulaire

Pour calculer $6^{73} \mod 100$, on a tout d'abord

$$73 = 2^0 + 2^3 + 2^6, \quad \rho_2(73) = 1001001.$$

i		0	1	2	3	4	5	6
$(6^{2^{i-1}})^2$			6^2	36^2	$(-4)^2$	16^2	56^2	36^2
6^{2^i}	mod 100	6	36	-4	16	56	36	-4

$6^{73} \mod 100 = 6^{2^0}.6^{2^3}.6^{2^6} = 6.16.(-4) = 16 \mod 100.$

6 élévations au carré et 2 produits dans $\mathbb{Z}_{100}$.
Bien plus efficace que 73 multiplications.

Dans `Mathematica` : `PowerMod[6,73,100]`

Complexité des opérations

Temps nécessaire pour réaliser des calculs (addition, produit, inversion,...) dans un champ fini au moyen d'un ordinateur.

simplifier : uniquement opérations élémentaires les opérations sur les bits (problèmes d'allocation mémoire...)

opérations supposées être réalisées en un temps constant (dépendant de l'ordinateur)

Complexité des opérations

Addition de deux entiers représentés en base 2.
(véritable processeur : puissance de 2)

report		1	1	1	1			
$\rho_2(120)$			1	1	1	1	0	0	0
$\rho_2(30)$	+				1	1	1	1	0
		1	0	0	1	0	1	1	0

Observation

pour chacune des colonnes, en commençant par la droite,

pour obtenir un bit s réponse (+ un bit r' de report),
on regarde 3 bits (un bit pour chacun des deux nombres, a et b, plus un bit r provenant d'un éventuel report).

Complexité des opérations

a	b	r	$\rightarrow$	s	r'
0	0	0		0	0
0	1	0		1	0
1	0	0		1	0
1	1	0		0	1
0	0	1		1	0
0	1	1		0	1
1	0	1		0	1
1	1	1		1	1

Conclusion

Le nombre d'opérations élémentaires sur les bits pour additionner deux entiers x et y est proportionnel à $\max(L_2(x), L_2(y))$, ou en $\mathcal{O}(\max(\ln x, \ln y))$.

Complexité des opérations

Multiplication de deux entiers 25×13

				1	1	0	0	1
$\times$					1	1	0	1
				1	1	0	0	1
		1	1	0	0	1		
+	1	1	0	0	1			
1	0	1	0	0	0	1	0	1

Chaque copie de 11001 est décalée d'un cran vers la gauche (un cran supplémentaire par zéro rencontré).

Conclusion

Pour multiplier x et y, on réalise, de proche en proche, au plus $L_2(y) - 1$ additions entre deux nombres de longueur $L_2(x)$.
Temps proportionnel à $L_2(x).L_2(y)$ ou en $\mathcal{O}(\ln x . \ln y)$

Complexité des opérations

Remarque

La division euclidienne se traite de manière semblable.

La division euclidienne (quotient et diviseur) d'un entier x tel que $L_2(x) = k$ par un entier y tel que $L_2(y) = \ell$ nécessite un nombre d'opérations élémentaires proportionnel à $\ell(k - \ell + 1)$.

Complexité des opérations

Algorithme d'Euclide

Soient $a, b \in \mathbb{Z}$ avec $a \neq 0$.

$$\begin{array}{rcll} b & = & a\,q_1 + r_1, & 0 < r_1 < a \\ a & = & r_1\,q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2\,q_3 + r_3 & 0 < r_3 < r_2 \\ & \vdots & & \\ r_{j-2} & = & r_{j-1}\,q_j + r_j & 0 < r_j < r_{j-1} \\ r_{j-1} & = & r_j\,q_{j+1}. & \end{array}$$

$\text{pgcd}(a, b) = r_j$. On pose $r_0 = a$.

Théorème de Bezout

Soient $a, b \in \mathbb{Z}$ tels que $ab \neq 0$. Il existe $\alpha_0, \beta_0 \in \mathbb{Z}$ tels que

$$\text{pgcd}(a, b) = a\,\alpha_0 + b\,\beta_0.$$

Complexité des opérations

Exemple

$$\begin{array}{rcl} 735 & = & 6.121 + 9 \\ 121 & = & 13.9 + 4 \\ 9 & = & 2.4 + 1 \\ 4 & = & 4.1 \end{array}$$

$\text{pgcd}(735, 121) = 1$, $1 = \alpha_0.121 + \beta_0.735$

$$\begin{array}{rcl} 1 & = & 9 - 2.4 \\ & = & 9 - 2.(121 - 13.9) = -2.121 + 27.9 \\ & = & -2.121 + 27.(735 - 6.121) = -164.121 + 27.735. \end{array}$$

Donc, dans $\mathbb{Z}_{735}$, $121^{-1} = -164 = 571$.

Complexité des opérations

L'algorithme d'Euclide étendu :
calcul simultané de $\text{pgcd}(a, b)$ et α_0, β_0
deux suites $(A_n)_{n\in\mathbb{N}}$ et $(B_n)_{n\in\mathbb{N}}$ t.q.

$$A_0 = 0,\ A_1 = 1,\ B_0 = 1,\ B_1 = 0,$$

et pour tout $n \geq 1$,

$$A_{n+1} = q_n A_n + A_{n-1} \ \text{ et } \ B_{n+1} = q_n B_n + B_{n-1}.$$

Proposition

$$r_n = (-1)^n A_{n+1}\,a + (-1)^{n+1} B_{n+1}\,b,\ \forall n \geq 0.$$

Complexité des opérations

On procède par récurrence sur n. Pour $n = 0$, OK : $r_0 = a$
Pour $n = 1$, on a

$$r_1 = -A_2\,a + B_2\,b = -q_1\,a + b.$$

Supposons OK pour les valeurs $< n$ et vérifions-le pour n.

$$\begin{array}{rcl} r_n & = & r_{n-2} - r_{n-1} q_n \\ & = & (-1)^n A_{n-1}\,a + (-1)^{n+1} B_{n-1}\,b - ((-1)^{n+1} A_n\,a + (-1)^n B_n\,b) q_n \\ & = & (-1)^n (A_{n-1} + A_n\,q_n)\,a + (-1)^{n+1} (B_{n-1} + B_n\,q_n)\,b \\ & = & (-1)^n A_{n+1}\,a + (-1)^{n+1} B_{n+1}\,b. \end{array}$$

Complexité des opérations

Exemple

Reprenons le pgcd de $a = 121$ et $b = 735$.

$q_1 = 6,\ q_2 = 13,\ q_3 = 2,\ q_4 = 4$ et $r_1 = 9,\ r_2 = 4,\ r_3 = 1,\ r_4 = 0.$

$$A_0 = 0,\ A_1 = 1,\ A_2 = q_1A_1 + A_0 = 6,$$
$$A_3 = q_2A_2 + A_1 = 79,\ A_4 = q_3A_3 + A_2 = 164,$$
$$B_0 = 1,\ B_1 = 0,\ B_2 = q_1B_1 + B_0 = 1,$$
$$B_3 = q_2B_2 + B_1 = 13,\ B_4 = q_3B_3 + B_2 = 27.$$

De là, par la proposition précédente, il vient

$$1 = r_3 = (-1)^3A_4\,121 + (-1)^4B_4\,735 = (-164).121 + 27.735.$$

Complexité des opérations

Remarque

Si $b > a > 0$, on peut montrer que
la complexité de l'algorithme d'Euclide est $\mathcal{O}(\ln b)$ et
pour la version étendue, on a $\mathcal{O}(\ln a.\ln b)$.

L'algorithme d'Euclide et sa version étendue peuvent facilement être adaptés au cas de deux polynômes.

Dans `Mathematica`, `GCD[121,735] = 1`
`ExtendedGCD[121,735] = {1, {-164,27}}`

Complexité des opérations

Opérations dans $\mathbb{F}_q$, $q = p^f$, $\mathbb{F}_q = \mathbb{F}_p/\langle M\rangle$ avec deg $M = f$

$$a_{f-1}X^{f-1} + \cdots + a_0, \quad a_i \in \mathbb{F}_p.$$

l'addition de 2 tels objets nécessite f sommes modulo p

$$[a_{f-1}X^{f-1} + \cdots + a_0] + [b_{f-1}X^{f-1} + \cdots + b_0]$$
$$= (\underbrace{a_{f-1} + b_{f-1}}_{(\mathrm{mod}\ p)})X^{f-1} + \cdots + (\underbrace{a_0 + b_0}_{(\mathrm{mod}\ p)}).$$

Coût

$a_i, b_i < p$. Donc la somme des deux éléments de $\mathbb{F}_q$ requiert $\mathcal{O}(f \ln p)$ opérations car la somme de deux nombres $< p$ se réalise (en base 2) en $\mathcal{O}(\ln p)$ opérations (nous admettrons que sur $\mathbb{F}_p$, les coûts sont semblables à ceux obtenus pour les développpements en base 2.)

Complexité des opérations

Une multiplication de 2 éléments de $\mathbb{F}_q$ est effectuée grâce à des additions et à des multiplications modulo p.
complexité addition $<<$ complexité multiplication
$\Rightarrow$ regarder uniquement le nombre de multiplications.

produit de deux polynômes P et Q de degré $< f$, $\mathcal{O}(f^2)$ multiplications de coefficients modulo p sont nécessaires :

$$[a_{f-1}X^{f-1}+\cdots+a_0].[b_{f-1}X^{f-1}+\cdots+b_0] = \sum_{j=0}^{2f-2} \underbrace{\left(\sum_{k+\ell=j} a_k.b_\ell\right)}_{(\mathrm{mod}\ p)} X^j.$$

Les produits $a_k.b_\ell$ apparaissent tous exactement une fois, $k, \ell \in \{0, \ldots, f-1\}$.

Complexité des opérations

Coût

chaque multiplication : $\mathcal{O}(\ln^2 p)$ opérations.
(Nous admettrons que sur $\mathbb{F}_p$, les coûts sont semblables à ceux obtenus en base 2 et puisque nous travaillons modulo p, cela revient à considerer le produit de 2 entiers $< p$.)

Le coût total de la multiplication est donc $\mathcal{O}(f^2 \ln^2 p) = \mathcal{O}(\ln^2 q)$.

le polynôme obtenu est de deg $\leq 2f-2$ et doit être réduit modulo M. Réaliser la division euclidienne de $P.Q$ par M emploie $\mathcal{O}(f)$ divisions d'entiers modulo p (une division se fait en $\mathcal{O}(\ln^2 p)$) et aussi $\mathcal{O}(f^2)$ multiplications d'entiers modulo p.

Ainsi la division prend un temps $\mathcal{O}(f^2 \ln^2 p) = \mathcal{O}(\ln^2 q)$.

Les deux étapes nécessitant le même ordre d'opérations, la complexité globaloe est encore d'ordre $\mathcal{O}(\ln^2 q)$

Complexité des opérations

Remarque

Effectuer une division dans $\mathbb{F}_q$ revient à multiplier par l'inverse.

réalisé grâce à l'algorithme d'Euclide étendu (adapté aux polynômes de $\mathbb{F}_p[X]$). On peut montrer que la recherche de l'inverse se fait en $\mathcal{O}(\ln^2 q)$ opérations élémentaires.

Remarque

Le calcul d'une puissance n-ième dans $\mathbb{F}_q$ peut se faire sur la même base que l'exponentiation modulaire.

Cela nécessite $\mathcal{O}(\ln n)$ multiplications dans $\mathbb{F}_q$.

Le coût total est $\mathcal{O}(\ln n . \ln^2 q)$.

A propos des nombres premiers

Proposition

Il existe une infinité de nombres premiers.

P.A. Supposons qu'il n'existe qu'un nombre fini de nombres premiers $2 = p_1 < \ldots < p_k$.

$N = p_1 \cdot p_2 \cdots p_k + 1 > p_k$ ne peut être premier.

N est composé et divisible par un nombre premier p_i.

De là, $1 = N - p_1 \cdot p_2 \cdots p_k$ doit donc être divisible par p_i !

A propos des nombres premiers

Corollaire

Soit p_k, le k-ième nombre premier. On a

$$p_k \leq 2^{2^{k-1}}.$$

En effet, tout nombre premier divisant $p_1 \cdots p_k + 1$ est distinct de $p_1, \ldots, p_k$. Ainsi, $p_{k+1} \leq p_1 \cdots p_k + 1$.

On procède alors par récurrence. On a $p_1 \leq 2$ et de là,

$$p_{k+1} \leq 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{k-1}} + 1 < 2^{2^k}.$$

En effet,

$$\underbrace{2.2}_{2\times}\underbrace{2.2.2.2}_{4\times} \cdots \underbrace{2 \cdots 2}_{2^{k-1}} = 2^{\sum_{i=1}^{k-1} 2^i} = 2^{2^k - 2}.$$

REMARQUE

On peut trouver des plages arbitrairement longues d'entiers consécutifs tous composés.

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+n+1.$$

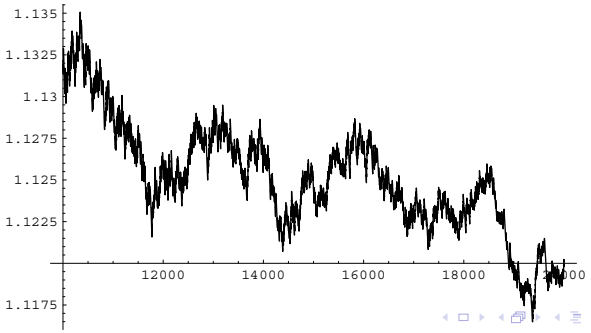
Par contre, il est conjecturé qu'il existe une infinité de nombres premiers jumeaux, i.e., tels que p et $p+2$ soient premiers.

THÉORÈMES DE RARÉFACTION DES NOMBRES PREMIERS

Si $\pi(n)$ = nombre de nombres premiers $\leq n$, alors

$$\lim_{n\to\infty} \frac{\pi(n)\ln n}{n} = 1 \qquad \text{,i.e.} \quad \frac{\pi(n)}{n} \sim \frac{1}{\ln n}.$$

Graphique de $\pi(n)\ \frac{\ln n}{n}$ pour $10^4 \leq n \leq 2.10^4$.



THÉORÈME DE DIRICHLET

Si a et b sont premiers entre eux, alors il existe une infinité de nombres premiers de la forme $a + n\,b$.

INFINITÉ DE NOMBRES PREMIERS DE LA FORME $4n+3$

P.A. Supposons qu'il n'existe qu'un nombre fini de nombres premiers $q_1 < \cdots < q_k$ de cette forme.

$$N = 4q_1q_2\cdots q_k - 1 = 4\,(q_1q_2\cdots q_k - 1)+3$$

N n'est PAS premier car $N > q_k$

- Aucun nombre premier, hormis 2, n'est de la forme $4n+2$ ou $4n$. Aucun facteur de ce type n'intervient dans la décomposition de N en facteurs premiers.
- N ne peut contenir dans sa décomposition uniquement des facteurs de la forme $4n+1$ car il serait alors lui-même de cette forme.

$\Rightarrow N$ doit contenir un facteur premier q_i de la forme $4n+3$.

$1 = 4q_1q_2\cdots q_k - N$ doit être divisible par q_i !

A PROPOS DES NOMBRES PREMIERS

Une progression arithmétique de nombres premiers de longueur ℓ : $\{p + k\,d \in \mathcal{P},\ k = 0, \ldots, \ell - 1\}$

$$199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089$$

BEN GREEN - TERENCE TAO (2004)

Pour tout ℓ, l'ensemble $\mathcal{P}$ des nombres premiers contient une progression arithmétique de longueur ℓ.

MATHÉMATIQUES DISCRÈTES (4)
CRYPTOGRAPHIE "CLASSIQUE"

Michel Rigo

http://www.discmath.ulg.ac.be/

Année 2007–2008

CRYPTOGRAPHIE. N. F.

Art d'écrire en chiffres ou d'une façon secrète quelconque.

Ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données, afin d'en préserver la confidentialité et l'authenticité.

EXEMPLE

"Mon numéro de carte VISA est le 1234-3552-1209-7633"

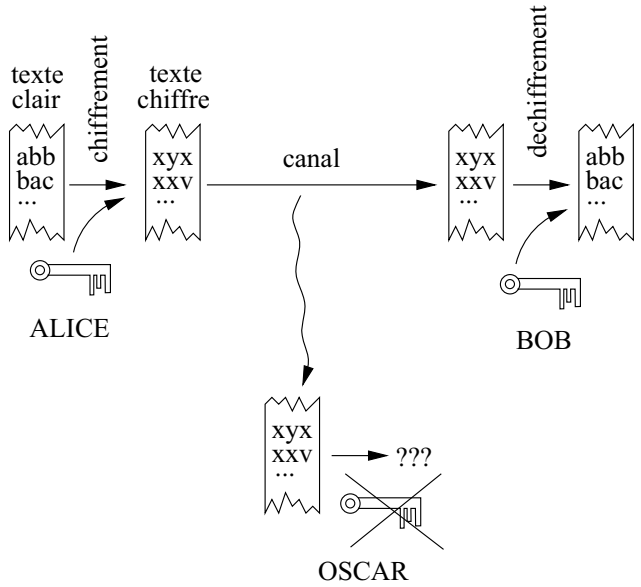
↓

"XFHEBBCASKOIUUSBCKKQHDGGDDSJQQIEUEU"

Applications

- Armée, gouvernement
- Banques, transactions bancaires, bancontact, ...
- Internet, paiement en ligne par carte de crédit, ...
- Vote électronique
- GSM (identification, code PIN)
- Télévision payante (à la carte)
- Signatures électroniques, recommandés électroniques, ...
- Mots de passe informatiques, ...

Les protagonistes...



Système cryptographique

Définition

cryptosystème $(\mathcal{P}, \mathcal{C}, \mathcal{K})$

- $\mathcal{P}$ est l'ensemble fini des textes clairs possibles (plaintexts),
- $\mathcal{C}$ est l'ensemble fini des textes chiffrés possibles (ciphertexts),
- $\mathcal{K}$ est l'ensemble fini des clés possibles, appelé parfois espace des clés (keys),
- Pour tout $k \in \mathcal{K}$, il existe une fonction de chiffrement (encryption rule) e_k t.q.

$$e_k : \mathcal{P} \to \mathcal{C} : t \mapsto e_k(t)$$

et $\exists$ une fonction de déchiffrement (decryption rule) d_k t.q.

$$d_k : \mathcal{C} \to \mathcal{P} : t \mapsto d_k(t) \quad \text{et} \quad \forall t \in \mathcal{P},\ d_k(e_k(t)) = t.$$

Système cryptographique

Remarque

Pour permettre le déchiffrage, la fonction e_k doit bien évidemment être injective pour tout $k \in \mathcal{K}$.

Exemple : chiffrement par décalage

Chiffrement par décalage

$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. $\forall k \in \{0, \ldots, 25\}$,

$$e_k(x) = (x + k) \mod 26 \quad \text{et} \quad d_k(y) = (y - k) \mod 26.$$

suite $\mathbf{x} = x_1 x_2 \cdots x_\ell$, $x_i \in \mathcal{P}$ chiffrée avec e_k ($k \in \mathcal{K}$ choisi de commun accord entre A et B), A transmet

$$\mathbf{y} = e_k(x_1) e_k(x_2) \cdots e_k(x_\ell).$$

Etape souvent préalable au chiffrement

Codage = ensemble des conventions pour modifier le texte clair en un texte équivalent plus simple à traiter du point de vue cryptographique.

Exemple : chiffrement par décalage

Codage "standard"

A veut transmettre le message "`bonsoir`", chaque lettre est remplacée par sa position dans l'alphabet $\Sigma = \{\mathtt{a}, \ldots, \mathtt{z}\}$

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

"`bonsoir`" est *codé* en "$\mathbf{x} = 1,14,13,18,14,8,17$".

codage : bijection entre l'alphabet Σ et $\{0, \ldots, 25\}$.

décodage : application inverse

Ne pas confondre : codage $\neq$ chiffrement.

Exemple : chiffrement par décalage

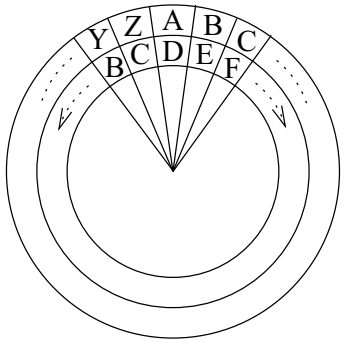
Fin de l'exemple...

Si la clé choisie est $k = 3$ (Jules César), alors

$$\begin{aligned}\mathbf{y} &= e_3(1) e_3(14) e_3(13) e_3(18) e_3(14) e_3(8) e_3(17) \\ &= 4, 17, 16, 21, 17, 11, 20.\end{aligned}$$

"`bonsoir`" $\longrightarrow$ "`erqvrlu`".

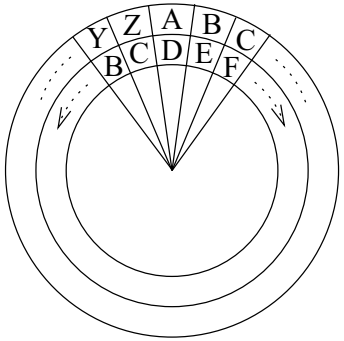
Exemple : chiffrement par décalage



Remarque

Cryptosystème peu sûr...

Exemple : chiffrement par décalage



Remarque

Cryptosystème peu sûr...

Exemple : chiffrement par décalage

2001 : l'odysée de l'espace, HAL

Principe de Kerckhoff

Définition

cryptanalyse= ensemble des moyens et techniques mis en oeuvre pour retrouver le texte clair ou au moins une certaine information contenue dans celui-ci.

Hypothèses de travail

Le principe de Kerckhoff suppose qu'Oscar connaît le cryptosystème utilisé.

La sécurité du système réside alors dans la protection de la clé k choisie par Alice et Bob.

Attaques

Types d'attaque dont dispose Oscar (par difficulté ↓)

- Texte chiffré connu : Oscar connaît uniquement un fragment de texte chiffré **y**.
- Texte clair connu : Oscar connaît un texte clair **x** et le texte chiffré **y** correspondant.
- Texte clair choisi : Oscar a accès à une machine chiffrante. Il peut choisir un texte clair **x** et obtenir le texte chiffré **y** correspondant.
- Fonction de chiffrement connue : Oscar connaît précisément la fonction utilisée pour le chiffrement. Son but est alors de découvrir la fonction de déchiffrement. Situation typique des cryptosystèmes à clé publique.
- Texte chiffré choisi : Oscar a temporairement accès à une machine déchiffrante. Il peut choisir un texte chiffré **y** et obtenir le texte clair **x** correspondant.

IMPLÉMENTATION

```
In[1]:= Characters["bonjour"]

Out[1]= {b, o, n, j, o, u, r}

In[2]:= StringJoin[{"a", "b", "c"}]

Out[2]= abc

In[3]:= Map[Sqrt[#] &, {4, 2, 9}]

Out[3]= {2, √2, 3}
```

IMPLÉMENTATION

code / decode

```
alphabet = {" ", "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o",
   "p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z", ",", ".", "'", ":", "?"};

code[mot_] := Map[Position[alphabet, #][[1, 1]] - 1 &, Characters[mot]]

texteclair = "le jour de ses onze ans, harry potter, un orphelin eleve par un
    oncle et une tante qui le detestent, voit son existence bouleversee.";

codetxclair = code[texteclair]

{12, 5, 0, 10, 15, 21, 18, 0, 4, 5, 0, 19, 5, 19, 0, 15, 14, 26, 5, 0, 1, 14, 19, 27, 0, 8, 1,
 18, 18, 25, 0, 16, 15, 20, 20, 5, 18, 27, 0, 21, 14, 0, 15, 18, 16, 8, 5, 12, 9, 14, 0, 5,
 12, 5, 22, 5, 0, 16, 1, 18, 0, 21, 14, 0, 15, 14, 3, 12, 5, 0, 5, 20, 0, 21, 14, 5, 0, 20, 1,
 14, 20, 5, 0, 17, 21, 9, 0, 12, 5, 0, 4, 5, 20, 5, 19, 20, 5, 14, 20, 27, 0, 22, 15, 9, 20, 0,
 19, 15, 14, 0, 5, 24, 9, 19, 20, 5, 14, 3, 5, 0, 2, 15, 21, 12, 5, 22, 5, 18, 19, 5, 5, 28}

decode[liste_] := StringJoin[Table[alphabet[[liste[[i]] + 1]], {i, 1, Length[liste]}]]

decode[codetxclair]

le jour de ses onze ans, harry potter, un orphelin eleve par un
  oncle et une tante qui le detestent, voit son existence bouleversee.
```

IMPLÉMENTATION

```
cesar[n_] := Mod[n + 3, 32]

codetxchiffre = cesar[codetxclair]

{15, 8, 3, 13, 18, 24, 21, 3, 7, 8, 3, 22, 8, 22, 3, 18, 17, 29, 8, 3, 4, 17,
 22, 30, 3, 11, 4, 21, 21, 28, 3, 19, 18, 23, 23, 8, 21, 30, 3, 24, 17, 3, 18,
 21, 19, 11, 8, 15, 12, 17, 3, 8, 15, 8, 25, 8, 3, 19, 4, 21, 3, 24, 17, 3, 18,
 17, 6, 15, 8, 3, 8, 23, 3, 24, 17, 8, 3, 23, 4, 17, 23, 8, 3, 20, 24, 12, 3, 15,
 8, 3, 7, 8, 23, 8, 22, 23, 8, 17, 23, 30, 3, 25, 18, 12, 23, 3, 22, 18, 17, 3,
 8, 27, 12, 22, 23, 8, 17, 6, 8, 3, 5, 18, 24, 15, 8, 25, 8, 21, 22, 8, 8, 31}

txchiffre = decode[codetxchiffre]

ohcmrxucghcvhvcrq'hcdqv:ckduu.csrwwhu:
  cxqcruskholqchohyhcsducxqcrqfohchwcxqhcwdqwhctxlcohcghwhvwhqw:
  cyrlwcvrqch,lvwhqfhcerxohyhuvhh?
```

IMPLÉMENTATION

Cryptanalyse ?

```
In[17]:= Count[{1, 2, 1, 1, 2}, 1]

Out[17]= 3

In[22]:= Count[Characters[texteclair], "e"]

Out[22]= 24

In[19]:= Map[Count[codetxclair, #] &, Table[i, {i, 0, 31}]]

Out[19]= {23, 4, 1, 2, 2, 24, 0, 0, 2, 4, 1, 0, 6, 0,
          11, 8, 3, 1, 7, 7, 10, 6, 3, 0, 1, 1, 1, 3, 1, 0, 0, 0}

In[18]:= Map[Count[codetxchiffre, #] &, Table[i, {i, 0, 31}]]

Out[18]= {0, 0, 0, 23, 4, 1, 2, 2, 24, 0, 0, 2, 4, 1,
          0, 6, 0, 11, 8, 3, 1, 7, 7, 10, 6, 3, 0, 1, 1, 1, 3, 1}
```

Fréquence d'apparition

fréquences d'apparition des différentes lettres apparaissant dans les textes écrits en français.

lettre	%
e	15,87
a	9,42
i	8,41
s	7,90
t	7,26
n	7,15
r	6,46
u	6,24
l	5,34

Codage par blocs

Définition

Unité fondamentale pour réaliser le codage d'une chaîne, non pas une lettre, mais un bloc de m lettres consécutives.

Un bloc $t_1 \cdots t_m$ de $m \geq 1$ entiers consécutifs < 32, représente un nombre n écrit en base 32 :

$$n = \sum_{j=1}^{m} t_j \, 32^{m-j}.$$

Bloc de longueur m représente un nombre $0 \leq n \leq 32^m - 1$.

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{32^m}$ et non plus $\mathbb{Z}_{32}$.

Codage par blocs

Remarque

Utiliser un codage dans lequel on considère des blocs de m éléments augmente la sécurité du cryptosystème.

Sur notre exemple, $\mathcal{K} = \mathbb{Z}_{32}$ passe à $\mathcal{K} = \mathbb{Z}_{32^m}$.

Puisque le nombre de clés augmente, une recherche exhaustive menée par Oscar prend beaucoup plus de temps

si $m = 5$, $32^5 \simeq 33 \times 10^6$ et en testant 1000 clés/seconde, un peu plus de 9 heures pour parcourir l'espace des clés.

Codage par blocs

Remarque

Si nous découpons le texte clair en tronçons de longueur m, il faudrait que ce texte soit de longueur divisible par m.

S'il ne l'était pas, on ajouterait au préalable des symboles à la fin du texte pour que sa longueur soit divisible par m.

Attention

Faille possible de sécurité !

Implémentation

```
ajout[liste_, m_] := PadRight[liste, Length[liste] + Mod[-Length[liste], m]]

codetxclair = ajout[codetxclair, 5]

{12, 5, 0, 10, 15, 21, 18, 0, 4, 5, 0, 19, 5, 19, 0, 15, 14, 26, 5, 0, 1, 14,
 19, 27, 0, 8, 1, 18, 18, 25, 0, 16, 15, 20, 20, 5, 18, 27, 0, 21, 14, 0, 15, 18,
 16, 8, 5, 12, 9, 14, 0, 5, 12, 5, 22, 5, 0, 16, 1, 18, 0, 21, 14, 0, 15, 14, 3,
 12, 5, 0, 5, 20, 0, 21, 14, 5, 0, 20, 1, 14, 20, 5, 0, 17, 21, 9, 0, 12, 5, 0,
 4, 5, 20, 5, 19, 20, 5, 14, 20, 27, 0, 22, 15, 9, 20, 0, 19, 15, 14, 0, 5, 24,
 9, 19, 20, 5, 14, 3, 5, 0, 2, 15, 21, 12, 5, 22, 5, 18, 19, 5, 5, 28, 0, 0, 0}

codebloc[liste_, m_] := Map[FromDigits[#, 32] &, Partition[liste, m]]

codetxclair = codebloc[codetxclair, 5]

{12747087, 22610053, 628320, 16214176, 1527648, 8440409, 540308, 5860373, 1469601
 8565038, 176310, 5259314, 702479, 14790816, 5898926, 5263406, 21135925, 9449632,
 4378803, 21150363, 736564, 638400, 6039156, 5704864, 2610565, 23251557, 6160384}

decodebloc[liste_, m_] := decode[Flatten[Map[IntegerDigits[#, 32, m] &, liste]]]

decodebloc[codetxclair, 5]

le jour de ses onze ans, harry potter, un orphelin eleve par un
  oncle et une tante qui le detestent, voit son existence bouleversee.
```

Implémentation

```
codetxchiffre = Mod[codetxclair + 12345678, 32^5]

{25092765, 1401299, 12973998, 28559854, 13873326, 20786087,
 12885986, 18206051, 27041694, 20910716, 12521988, 17604992, 13048157,
 27136494, 18244604, 17609084, 33481603, 21795310, 16724481, 33496041,
 13082242, 12984078, 18384834, 18050542, 14956243, 2042803, 18506062}

decodebloc[codetxchiffre, 5]

w'xt'ajxnslk''n,gronmglenszj'glig?bqkskcyyg.:s:ds.k:dpdpyhl lnfj'
  y.donqlx?.pylk.?'x.ctydono:lpa?:f?ilogtbllgxnqqa:bqf,onnhmvsa:j'sqtxjn

decodebloc[Mod[codetxchiffre - 12345678, 32^5], 5]

le jour de ses onze ans, harry potter, un orphelin eleve par un
  oncle et une tante qui le detestent, voit son existence bouleversee.
```

Implémentation

`code[mot]`	chaîne de longueur n $\mapsto$ liste de n éléments de $\mathbb{Z}_{32}$
`decode[liste]`	liste de n éléments de $\mathbb{Z}_{32}$ $\mapsto$ chaîne de longueur n
`ajout[liste,m]`	liste quelconque $\mapsto$ liste de longueur divisible par m
`codebloc[liste,m]`	liste de $n.m$ éléments de $\mathbb{Z}_{32}$ $\mapsto$ liste de n éléments de $\mathbb{Z}_{32^m}$
`decodebloc[liste,m]`	liste de n éléments de $\mathbb{Z}_{32^m}$ $\mapsto$ chaîne de longueur $n.m$.

Quelques cryptosystèmes classiques

Chiffrement par substitution

Si $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{32}$, alors $\mathcal{K}$ est l'ensemble des permutations de $\{0, \ldots, 31\}$, i.e.,

$$\mathcal{K} = \{\nu \in \mathcal{S}_{32} \mid \nu : \mathbb{Z}_{32} \to \mathbb{Z}_{32} \text{ bijection}\}.$$

pour la clé $k = \nu$, on a

$$e_k(x) = \nu(x) \quad \text{et} \quad d_k(y) = \nu^{-1}(y).$$

Remarque

Par rapport au chiffrement par décalage, $\#\mathcal{K}$ est grand : $32! \simeq 2,6 \times 10^{35}$.

Quelques cryptosystèmes classiques

Chiffrement par substitution

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
e	:	d	k	,	l	p	n		q	x	f	s	z	.	u

p	q	r	s	t	u	v	w	x	y	z	,	.	’	:	?
’	a	c	i	g	?	t	v	o	y	w	r	b	m	j	h

le jour de ses onze ans, harry potter, un orphelin eleve par un oncle et une tante qui le detestent, voit son existence bouleversee.

slexu ?ce,leilieu.wle :.i,e :ccye’ugglc,e ?.euc’ lsq.elsltle’ :c e ?.eu.kslelge ?.leg :.glea ?qesle,lgligl.g,etuqgeiu.eloqigl.kl edu ?sltlcillb

Quelques cryptosystèmes classiques

Chiffrement par substitution

Nombre de clés important, mais ce cryptosystème est cassé en effectuant une analyse des fréquences : rechercher les lettres apparaissant le plus souvent, mais aussi les couples ou les triplets.

Ce cryptosystème NE peut être considéré comme sûr.

Seul intérêt : cryptogrammes dans les livres de jeux.

Quelques cryptosystèmes classiques

Chiffrement affin

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Soient $a, b \in \mathbb{Z}_n$ avec $pgcd(a, n) = 1$.

$$\mathcal{K} = \{(a, b) \mid a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$$

et pour une clé $k = (a, b)$ choisie dans $\mathcal{K}$, on a

$$e_k(x) = ax + b \mod n \quad \text{et} \quad d_k(y) = a^{-1}(y - b) \mod n.$$

a inversible pour que e_k soit injective.

Le nombre de clés est $n\,\varphi(n)$.

Quelques cryptosystèmes classiques

```
texteclair = "ving minutes plus tard, harry sortit
du magasin de hiboux avec une grande cage a
l'interieur de laquelle une magnifique chouette aux
plumes blanches comme la neige dormait
paisiblement.";
```

$k = (13, 8)$

decode[Mod[13 code[texteclair]+8, 32]]

```
"f' :chq' :yli ?hxdy ?hlur.gpurrmh ?krl'lh.yhqucu ?'
:h.ihp'bky hufiohy :ihcru :.ihoucihuhda' :lir'iyr
h.ihdueyiddihy :ihquc :'v'eyihopkyillihuy hxdyqi
?hbdu :opi ?hokqqihduh :i'cih.krqu'lhxu'?'bdiqi :lt"
```

Remarque

Cas particulier de chiffrement par substitution.
cryptanalyse : analyse statistique des fréquences d'apparition des lettres.

Quelques cryptosystèmes classiques

Monoalphabétique vs. polyalphabétique

Les chiffrements par décalage, par substitution et affin sont monoalphabétiques.

e_k s'applique à un seul élément de $\mathcal{P}$ à la fois (une lettre, un élément de $\mathbb{Z}_{32}$)

à chaque élément de $\mathcal{P}$ est appliquée la même fonction de chiffrement.

Pour un bloc de m symboles, aussi un système monoalphabétique car $\mathcal{P} = \mathbb{Z}_{32^m}$

Le chiffrement de Vigenère (Blaise de Vigenère, XVIè siècle) est polyalphabétique car il traite m symboles simultanément.

Quelques cryptosystèmes classiques

Chiffrement de Vigenère

Il s'agit en quelque sorte de m chiffrements par décalage, $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{32})^m$, si $k = (k_1, \ldots, k_m) \in (\mathbb{Z}_{32})^m$, alors

$$e_k(x_1, \ldots, x_m) = (x_1 + k_1, \ldots, x_m + k_m) \mod 32$$

$$d_k(y_1, \ldots, y_m) = (y_1 - k_1, \ldots, y_m - k_m) \mod 32.$$

Pour chiffrer une suite de longueur $rm + s$ de $\mathbb{Z}_{32}$, $0 \leq s < m$,

$$\mathbf{x} = x_1 \cdots x_m \,|\, \cdots \,|\, x_{(r-1)m+1} \cdots x_{rm} \,|\, x_{rm+1} \cdots x_{rm+s},$$

on calculera

$$\begin{aligned}\mathbf{y} \;=\; & (x_1 + k_1) \cdots (x_m + k_m) \,|\, \cdots \,|\, (x_{(r-1)m+1} + k_1) \cdots (x_{rm} + k_m) \,| \\ & (x_{rm+1} + k_1) \cdots (x_{rm+s} + k_s) \mod 32.\end{aligned}$$

Quelques cryptosystèmes classiques

L'implémentation est très simple

```
In[2]:= PadRight[{1, 2}, 10, {5, 3, 7}]

Out[2]= {1, 2, 7, 5, 3, 7, 5, 3, 7, 5}
```

Quelques cryptosystèmes classiques

```
texteclair = "ving minutes plus tard,harry sortit du magasin de
    hiboux avec une grande cage a l'interieur de laquelle une magnifique
    chouette aux plumes blanches comme la neige dormait paisiblement.";

codetxclair = code[texteclair];

Shallow[codetxclair]

{22, 9, 14, 7, 0, 13, 9, 14, 21, 20, <<174>>}

vigenere[liste_, cle_] := Mod[liste + PadRight[cle, Length[liste], cle], 32]

codetxchiffre = vigenere[codetxclair, {10, 8, 20}]

{0, 17, 2, 17, 8, 1, 19, 22, 9, 30, 13, 7, 10, 24, 0, 31, 27, 20, 30, 9, 6, 14, 3, 28,
 26, 6, 3, 8, 7, 25, 26, 8, 19, 28, 20, 14, 29, 20, 23, 9, 27, 11, 27, 29, 24, 8, 24,
 15, 8, 28, 19, 10, 3, 31, 0, 20, 11, 30, 25, 13, 8, 9, 24, 13, 20, 17, 26, 21, 24, 12,
 25, 10, 11, 21, 17, 13, 20, 11, 8, 0, 7, 17, 2, 30, 13, 6, 19, 13, 9, 28, 8, 24, 15,
 8, 0, 11, 25, 9, 15, 20, 0, 15, 8, 9, 24, 13, 20, 23, 9, 27, 24, 17, 26, 19, 25, 9,
 15, 8, 23, 18, 23, 9, 15, 28, 8, 15, 8, 21, 31, 0, 20, 26, 20, 9, 23, 13, 7, 10, 10,
 0, 11, 22, 23, 18, 13, 7, 10, 11, 3, 23, 21, 25, 10, 20, 21, 10, 22, 25, 19, 15, 25,
 10, 12, 3, 28, 21, 21, 19, 28, 20, 26, 9, 29, 29, 17, 22, 22, 13, 1, 15, 22, 8, 6}

decode[codetxchiffre]

 qbqhasvi:mgjx ?,t:ifnc.kzfchgyzhs.tn'twi,k,'xhxoh.sjc? tk:
  ymhixmtqzuxlyjkuqmtkh gqb:mfsmi.hxoh kyiot ohixmtwi,xqzsyiohwrwio.
  hohu? tztiwmgjj kvwrmgjkcwuyjtujvysoyjlc.uus.tzi''qvvmaovhf
```

Quelques cryptosystèmes classiques

Pour le déchiffrement...

```
vigenere[codetxchiffre, -{10, 8, 20}]
```

```
{22, 9, 14, 7, 0, 13, 9, 14, 21, 20, 5, 19, 0, 16, 12, 21, 19, 0, 20, 1, 18, 4, 27, 8,
 25, 0, 19, 15, 18, 20, 9, 20, 0, 4, 21, 0, 13, 1, 7, 1, 19, 9, 14, 0, 4, 5, 0, 8, 9, 2,
 21, 24, 0, 1, 22, 5, 3, 0, 21, 14, 5, 0, 7, 18, 1, 14, 4, 5, 0, 3, 1, 7, 5, 0, 1, 0, 12
 29, 9, 14, 20, 5, 18, 9, 5, 21, 18, 0, 4, 5, 0, 12, 1, 17, 21, 5, 12, 12, 5, 0, 21, 14
 5, 0, 13, 1, 7, 14, 9, 6, 9, 17, 21, 5, 0, 3, 8, 15, 21, 5, 20, 20, 5, 0, 1, 21, 24, 0,
 16, 12, 21, 13, 5, 19, 0, 2, 12, 1, 14, 3, 8, 5, 19, 0, 3, 15, 13, 13, 5, 0, 12, 1, 0,
 5, 9, 7, 5, 0, 4, 15, 18, 13, 1, 9, 20, 0, 16, 1, 9, 19, 9, 2, 12, 5, 13, 5, 14, 20, 28
```

Remarques

Dans le chiffrement de Vigenère, un même symbole peut être transformé en m symboles distincts suivant la position qu'occupe ce symbole dans un m-uple donné.

Cryptanalyse : test de Kasiski / indice de coïncidence

Quelques cryptosystèmes classiques

Chiffrement de Hill, Lester S. Hill (1929)

Cryptosystème polyalphabétique. $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{32})^m$ et

$$\mathcal{K} = GL_m(\mathbb{Z}_{32}),$$

l'ensemble des matrices inversibles à coefficients dans $\mathbb{Z}_{32}$.

Proposition

Une matrice carrée A à coefficients dans $\mathbb{Z}_n$ est inversible, i.e., il existe B tel $AB = BA = I$, SSI $\det(A)$ est inversible dans $\mathbb{Z}_n$.

Quelques cryptosystèmes classiques

règle des mineurs :

$$A\,\widetilde{\mathrm{cof}(A)} = \det A\; I = \widetilde{\mathrm{cof}(A)}\,A$$

$\mathrm{cof}(A)$: matrice des cofacteurs (ou mineurs algébriques) de A.

$\Leftarrow$. Si $\det A$ est inversible, l'inverse de A est $\widetilde{\mathrm{cof}(A)}$.

$\Rightarrow$. Si A est inversible et d'inverse A^{-1}, alors

$$1 = \det(AA^{-1}) = \det A \det A^{-1}$$

ce qui montre que $\det A$ est inversible.

Quelques cryptosystèmes classiques

Chiffrement de Hill

Si $k = (a_{ij}) \in GL_m(\mathbb{Z}_{32})$,
$e_k : \mathbb{Z}_{32}^m \to \mathbb{Z}_{32}^m : (x_1, \ldots, x_m) \mapsto (y_1, \ldots, y_m)$ est donné par

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

Quelques cryptosystèmes classiques

Chiffrement/Déchiffrement

La matrice A détermine une bijection $x \mapsto Ax$ de $(\mathbb{Z}_n)^m$ dans lui-même SSI A inversible.

$\Leftarrow$ Si $Ax = Ay$, en multipliant par A^{-1} : $x = y$ (injectif).
(surjectif) $\forall y \in (\mathbb{Z}_n)^m$, $x = A^{-1}y$ est tel que $Ax = y$.

$\Rightarrow$ $x \mapsto Ax$ est surjectif, pour tout e_i, $i = A, \ldots, m$, il existe un vecteur colonne C_i tel que $AC_i = e_i$. De là, la matrice dont les colonnes sont $C_1, \ldots, C_m$ est inverse de A.

Quelques cryptosystèmes classiques

```
texteclair = "le phenix sur lequel a ete preleve la plume qui se trouve dans
    votre baguette a egalement fourni une autre plume a une autre baguette.";

codetxclair = ajout[code[texteclair], 2];

Shallow[codetxclair]

{12, 5, 0, 16, 8, 5, 14, 9, 24, 0, <<124>>}

a = {{5, 17}, {4, 21}};

MatrixForm[a]
```

$$\begin{pmatrix} 5 & 17 \\ 4 & 21 \end{pmatrix}$$

```
hill[a_, liste_] := Flatten[Map[Mod[a.# , 32] &, Partition[liste, Length[a]]]]

codetxchiffre = hill[a, codetxclair]

{17, 25, 16, 16, 29, 9, 31, 21, 24, 0, 4, 5, 26, 8, 17, 25, 26, 29, 5, 16, 17, 21,
 21, 9, 25, 25, 16, 16, 15, 17, 17, 25, 3, 1, 12, 28, 5, 4, 28, 28, 6, 5, 25, 20,
 26, 29, 13, 4, 20, 21, 20, 4, 25, 3, 31, 2, 25, 20, 5, 5, 9, 7, 22, 14, 31, 0, 15,
 17, 2, 10, 28, 23, 30, 29, 24, 20, 25, 20, 5, 4, 16, 7, 17, 0, 22, 5, 7, 26, 4, 16,
 29, 19, 27, 14, 31, 21, 5, 25, 27, 1, 17, 21, 29, 24, 15, 17, 16, 16, 1, 9, 22, 29,
 17, 21, 5, 25, 27, 1, 17, 21, 29, 24, 15, 17, 2, 10, 28, 23, 30, 29, 24, 20, 21, 0}
```

Quelques cryptosystèmes classiques

```
Inverse[a, Modulus → 32]

{{17, 3}, {12, 1}}

hill[Inverse[a, Modulus → 32], codetxchiffre]

{12, 5, 0, 16, 8, 5, 14, 9, 24, 0, 19, 21, 18, 0, 12, 5, 17, 21, 5, 12, 0, 1, 0, 5, 20, 5, 0,
 18, 5, 12, 5, 22, 5, 0, 12, 1, 0, 16, 12, 21, 13, 5, 0, 17, 21, 9, 0, 19, 5, 0, 20, 18, 15,
 21, 22, 5, 0, 4, 1, 14, 19, 0, 22, 15, 20, 18, 5, 0, 2, 1, 7, 21, 5, 20, 20, 5, 0, 1, 0, 5,
 7, 1, 12, 5, 13, 5, 14, 20, 0, 6, 15, 21, 18, 14, 9, 0, 21, 14, 5, 0, 1, 21, 20, 18, 5, 0,
 16, 12, 21, 13, 5, 0, 1, 0, 21, 14, 5, 0, 1, 21, 20, 18, 5, 0, 2, 1, 7, 21, 5, 20, 20, 5, 28
```

Quelques cryptosystèmes classiques

Pour trouver cet inverse manuellement, on calcule $\det A = 5$, son inverse modulo 32 grâce à l'algorithme d'Euclide étendu, $(\det A)^{-1} = 13$ et enfin, la matrice des cofacteurs transposée,

$$\widetilde{\operatorname{cof} A} = \begin{pmatrix} 21 & -17 \\ -4 & 5 \end{pmatrix}.$$

On trouve,

- $13.21 = 273 \equiv 17 \mod 32$,
- $13.(-17) = -221 \equiv 3 \mod 32$,
- $13.(-4) = -52 \equiv 12 \mod 32$,
- $13.5 = 65 \equiv 1 \mod 32$.

CRYPTANALYSE DU CHIFFREMENT

cas où un texte clair de longueur m^2 est connu. Si Oscar connaît la valeur $m = 2$, le texte clair $12, 5, 0, 16$ et le texte chiffré correspondant $17, 25, 16, 16$, alors il en déduit que

$$A \underbrace{\begin{pmatrix} 12 & 0 \\ 5 & 16 \end{pmatrix}}_{B} = \begin{pmatrix} 17 & 16 \\ 25 & 16 \end{pmatrix}.$$

Pas de chance B n'est pas inversible, $\det(B) = 0$.

Oscar doit construire une matrice inversible dont les colonnes correspondent à des couples de texte clair lorsque ce dernier est décomposé en m-uples consécutifs.

CRYPTANALYSE DU CHIFFREMENT

On peut par exemple prendre pour premier couple $(12, 5)$ correspondant au texte chiffré $(17, 25)$ et comme second couple $(19, 21)$ qui correspond à $(4, 5)$

$$A \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix} = \begin{pmatrix} 17 & 4 \\ 25 & 5 \end{pmatrix}.$$

Puisque

$$\det \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix} \equiv 29 \mod 32, \quad A = \begin{pmatrix} 17 & 4 \\ 25 & 5 \end{pmatrix} \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix}^{-1}$$

et Oscar retrouve A.

CHIFFREMENT PAR PERMUTATION

Cas particulier du chiffrement de Hill, matrice pour le chiffrement : une matrice de permutation P.

Le chiffrement de Hill revient alors à permuter les lettres d'un même m-uple au moyen de la permutation définie par P.


```
p = {{0, 1, 0}, {0, 0, 1}, {1, 0, 0}}

{{0, 1, 0}, {0, 0, 1}, {1, 0, 0}}

decode[hill[p, codetxclair]]

e lhepixnsu  lrquel e eae trepevl le pauml qei ue srotveuda s
  notve ragbetue t eaalgmeet noufnirun  aetru peuml aeun  aetru beguatte
```

Quelques cryptosystèmes classiques

Chiffrement par flot, un exemple

on génère une suite de clés $\mathbf{z} = z_1 z_2 \cdots$ utilisées successivement pour chiffrer une suite $\mathbf{x} = x_1 x_2 \cdots$.

Soient $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{32}$. Pour chiffrer

$$\mathbf{x} = x_1 x_2 x_3 \cdots, \quad \forall i \geq 1,\ x_i \in \mathcal{P}$$

avec une clé k fixée initialement, on procède comme suit :

$$\mathbf{y} = (x_1 + k)(x_2 + x_1)(x_3 + x_2) \cdots \mod 32.$$

Revient à ajouter à la suite $\mathbf{x}$, la suite décalée d'une unité vers la droite.

Quelques cryptosystèmes classiques

```
texteclair = "essayer un chapeau valait beaucoup mieux que d'etre oblige de jeter ur
    sort,mais il aurait prefere ne pas avoir a le faire devant tout le monde.";

codetxclair = code[texteclair]

{5, 19, 19, 1, 25, 5, 18, 0, 21, 14, 0, 3, 8, 1, 16, 5, 1, 21, 0, 22, 1, 12, 1, 9,
 20, 0, 2, 5, 1, 21, 3, 15, 21, 16, 0, 13, 9, 5, 21, 24, 0, 17, 21, 5, 0, 4, 29, 5,
 20, 18, 5, 0, 15, 2, 12, 9, 7, 5, 0, 4, 5, 0, 10, 5, 20, 5, 18, 0, 21, 14, 0, 19,
 15, 18, 20, 27, 13, 1, 9, 19, 0, 9, 12, 0, 1, 21, 18, 1, 9, 20, 0, 16, 18, 5, 6, 5,
 18, 5, 0, 14, 5, 0, 16, 1, 19, 0, 1, 22, 15, 9, 18, 0, 1, 0, 12, 5, 0, 6, 1, 9, 18,
 5, 0, 4, 5, 22, 1, 14, 20, 0, 20, 15, 21, 20, 0, 12, 5, 0, 13, 15, 14, 4, 5, 28}

flot[liste_, k_] := Mod[Drop[Prepend[liste, k], -1] + liste, 32]

flot[codetxclair, 5]

{10, 24, 6, 20, 26, 30, 23, 18, 21, 3, 14, 3, 11, 9, 17, 21, 6, 22, 21, 22, 23, 13, 13, 10,
 29, 20, 2, 7, 6, 22, 24, 18, 4, 5, 16, 13, 22, 14, 26, 13, 24, 17, 6, 26, 5, 4, 1, 2,
 25, 6, 23, 5, 15, 17, 14, 21, 16, 12, 5, 4, 9, 5, 10, 15, 25, 25, 23, 18, 21, 3, 14, 19,
 2, 1, 6, 15, 8, 14, 10, 28, 19, 9, 21, 12, 1, 22, 7, 19, 10, 29, 20, 16, 2, 23, 11, 11,
 23, 23, 5, 14, 19, 5, 16, 17, 20, 19, 1, 23, 5, 24, 27, 18, 1, 1, 12, 17, 5, 6, 7, 10,
 27, 23, 5, 4, 9, 27, 23, 15, 2, 20, 20, 3, 4, 9, 20, 12, 17, 5, 13, 28, 29, 18, 9, 1}

decode[%]

jxftz:wrucnckiqufvuvwmmj'tbgfvxrdepmvnzmxqfzedabyfweoqnupledіejoyywrucnsbafohnj.
  siulavgsj'tpbwkkwwensepqtsawex,raalqefgj,wedi,wobttcditlqem.'ria
```

Quelques cryptosystèmes classiques

Définition

chiffrement par flot : $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F})$

- $\mathcal{L}$ ensemble fini : alphabet du flot de clés,
- $\mathcal{F}$ suite de fonctions $(f_n)_{n\geq 1}$: générateur du flot de clés t.q.

$$\forall n \geq 1, \quad f_n : \mathcal{K} \times \mathcal{P}^{n-1} \to \mathcal{L},$$

- $\forall z \in \mathcal{L}, \exists\ e_z : \mathcal{P} \to \mathcal{C}$ et $d_z : \mathcal{C} \to \mathcal{P}$ t.q. $d_z(e_z(x)) = x,\ \forall x$

A une suite $\mathbf{x} = x_1 x_2 x_3 \cdots$ d'éléments de $\mathcal{P}$ et à une clé $k \in \mathcal{K}$, correspond une unique suite de fonctions $\mathcal{F} = (f_1, f_2, f_3, \ldots)$.

Chaque f_n donne un $z_n \in \mathcal{L}$ et à ce z_n, il correspond e_{z_n} et d_{z_n}.

Le chiffrement de $\mathbf{x}$ est $e_{z_1}(x_1) e_{z_2}(x_2) e_{z_3}(x_3) \cdots$

Quelques cryptosystèmes classiques

Pour notre exemple

$e_{z_1}(x_1) = x_1 + k \pmod{32}$ et
pour $n > 1$, $e_{z_n}(x_n) = x_n + x_{n-1} \pmod{32}$.

cas très particulier de chiffrement par flot.

En toute généralité, un chiffrement par flot admet plus de souplesse.

Definition

Un chiffrement en chaîne est dit synchrone si la suite de clés $(z_n)_{n\geq 1}$ est indépendante du texte clair.

Un chiffrement est dit (ultimement) périodique si la suite $(z_n)_{n\geq 1}$ est (ultimement) périodique, i.e., s'il existe $N, p \geq 1$ tels que $z_n = z_{n+p}$ pour tout $n \geq N$.

DES - AES

Tous les chiffrements rencontrés jusqu'à présent sont à clé secrète (ou privée), i.e., la sécurité du système réside dans la non-divulgation de la clé $k \in \mathcal{K}$ choisie.

Les systèmes rencontrés sont aisément cryptanalysés.

DES : cryptosystème à clé secrète considéré jusqu'il y a peu comme sûr

Data Encryption Standard développé initialement par IBM (1977) comme une variante de LUCIFER.

DES - AES

Les cryptosystèmes à clé secrète (décalage, substitution, Hill, Vigenère) sont idempotents : *composer successivement deux cryptosystèmes du même type est encore un chiffrement de même type*
$\Rightarrow$ aucun intérêt à l'itérer

DES n'est pas idempotent (on le construit sur le produit de deux systèmes qui ne commutent pas).
$\Rightarrow$ La sécurité est augmentée en l'itérant. Ici, $16\times$

DES - AES

Clé de 64 bits

suite aléatoire s de 56 bits, $s = s_1 \cdots s_{56} \in \{0,1\}^{56}$.
On définit une suite de 64 bits $k = k_1 \cdots k_{64}$ t.q.

$$k_1, \ldots, k_7, k_9, \ldots, k_{15}, \ldots, k_{57}, \ldots, k_{63} = s_1, \ldots, s_{56}$$

et

$$\forall j \in \{0, \ldots, 7\}, \quad \sum_{i=1}^{8} k_{j8+i} \equiv 1 \mod 2.$$

Cette condition stipule simplement que la somme de 8 bits consécutifs est toujours impaire (détecter une erreur dans le stockage ou le transfert, bit de parité).

Ces 8 bits ajoutés aux 56 bits de départ ne jouent pas de rôle dans la suite.

DES - AES

On considère un texte clair de 64 bits $\mathbf{x} = x_1 \cdots x_{64} \in \{0,1\}^{64}$.
On lui applique une permutation ν de $\{1, \ldots, 64\}$:

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Ainsi, on considère $\nu(\mathbf{x}) = x_{\nu(1)} \cdots x_{\nu(64)} = x_{58}\, x_{50} \cdots x_7$.
Ce mot $\nu(\mathbf{x})$ est divisé en deux mots de longueur 32,

$$\nu(\mathbf{x}) = L_0 R_0 = \left(x_{\nu(1)} \cdots x_{\nu(32)}\right) \left(x_{\nu(33)} \cdots x_{\nu(64)}\right).$$

DES - AES

Connaissant L_n et R_n ($n \geq 0$), on calcule L_{n+1} et R_{n+1}

$$L_{n+1} = R_n \tag{1}$$

$$R_{n+1} = L_n \oplus f(R_n, K_{n+1}) \tag{2}$$

où $\oplus$ représente le "ou-exclusif",

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

Jusqu'à obtenir le mot $L_{16}R_{16}$.

Le chiffrement de **x** est $\mathbf{y} = \nu^{-1}(L_{16}R_{16})$. On dit qu'on applique le DES en seize tours.

DES - AES

Comment obtenir les clés $K_1, \ldots, K_{16}$ (processus de diversification des clés) et la fonction f.

On définit d'abord K_0. On l'obtient à partir de k en sélectionnant dans l'ordre les bits (on ne prend pas en compte ici les bits de parité k_{j8}, $j = 1, \ldots, 8$) de k en suivant la permutation

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36

pour former une chaîne de longueur 28 : $C_0 = k_{57}\, k_{49} \cdots k_{44}\, k_{36}$ et aussi la permutation

63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

pour former une 2ème chaîne de longueur 28 : $D_0 = k_{63}\, k_{55} \cdots k_{12}\, k_4$. Ainsi, $K_0 = C_0 D_0$.

DES - AES

Pour construire K_{n+1}, $n \geq 0$, on procède en deux étapes. Disposant de C_n et D_n, on construit C_{n+1} et D_{n+1} en effectuant une permutation circulaire d'une ou de deux unités vers la gauche sur C_n et D_n de la manière suivante

$n+1$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
# permut.	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

$$C_1 = k_{49}\, k_{41} \cdots k_{44}\, k_{36}\, k_{57},\ C_2 = k_{41} \cdots k_{44}\, k_{36}\, k_{57}\, k_{49},\ \ldots$$

$$D_1 = k_{55}\, k_{47} \cdots k_{12}\, k_4\, k_{63},\ D_2 = k_{47} \cdots k_{12}\, k_4\, k_{63}\, k_{55},\ \ldots.$$

On obtient K_n en sélectionnant 48 des 56 bits de C_nD_n dans l'ordre suivant

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

DES - AES

Passons à la définition de f qui prend comme argument un bloc R_n de 32 bits et une clé K_{n+1} de 48 bits pour produire un bloc de 32 bits.
On remplace R_n par un bloc R'_n de 48 bits en recopiant certains des bits de R_n plusieurs fois de la manière suivante (on parle de l'expansion de R_n)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

DES - AES

Ainsi, si R_n est de la forme $r_1 r_2 \cdots r_{32}$, on obtient la suite

$$R'_n = r_{32}\, r_1\, r_2\, r_3\, r_4\, r_5\, r_4\, r_5 \cdots r_{31}\, r_{32}\, r_1.$$

On additionne à présent bit à bit R'_n et K_{n+1} modulo 2 pour obtenir B et cette suite est alors découpée en 8 blocs de 6 bits, i.e.,

$$B = R'_n \oplus K_{n+1} = \underbrace{b_1 \cdots b_6}_{B_1}\ \underbrace{b_7 \cdots b_{12}}_{B_2} \cdots \underbrace{b_{43} \cdots b_{48}}_{B_8}.$$

DES - AES

Transformer chacun des 8 blocs en 8 nouveaux blocs B'_i de longueur 4. La valeur de la fonction f est une permutation de $B'_1 \cdots B'_8$ qui est bien de longueur 32 : $\mu(B'_1 \cdots B'_8)$..
La transformation de B_i en B'_i est réalisée par une table S_i.

S_1 :

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

On l'utilise pour calculer B'_1 à partir de $B_1 = b_1 b_2 b_3 b_4 b_5 b_6$. Le mot $b_1 b_6$ (resp. $b_2 b_3 b_4 b_5$) représente un entier $0 \leq x \leq 3$ (resp. $0 \leq y \leq 15$) écrit en base 2. Dans le tableau S_1, on considère l'élément $(S_1)_{x,y}$ se trouvant à la ligne x et à la colonne y. La représentation binaire de $(S_1)_{x,y}$ (éventuellement complétée par des zéros de tête pour obtenir un mot de longueur 4) est alors B'_1. On procède de manière semblable pour $B'_2, \ldots, B'_8$ avec les tables données ci-après. La dernière table reprend la permutation μ.

DES - AES

Exemple

Soit $B_1 = 100101$. Le mot $b_1 b_6 = 11$ (resp. $b_2 b_3 b_4 b_5 = 0010$) correspond à $x = 3$ (resp. $y = 2$). Dans la table S_1, cela correspond[1] à l'élément 8 dont la représentation binaire est 0100 qui est B'_1.

[1] Les lignes sont numérotées de 0 à 3 et les colonnes de 0 à 15.

DES - AES

Les tables S sont appelées S-boxes (ou substitution-boxes) : composantes non linéaires du cryptosystème. Aucune des boîtes n'est une fonction linéaire ou affine.

Avantage certain : rapidité. Implémentation réalisée de manière efficace logiciellement ou physiquement sur des circuits électroniques élémentaires à faible coût (exemple, placés sur une carte de crédit).

Critique principale : espace des clés de taille $2^{56} \simeq 7,2 \times 10^{16}$ jugée trop petite. En effet, en 1993, on estimait pouvoir construire une puce capable de tester 5×10^7 clés par seconde pour un coût proche de 8 euros. Ainsi, en regroupant un grand nombre de telles puces, on pourrait trouver la clé secrète en quelques heures.

DES - AES

S_2 :

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3 :

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4 :

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5 :

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

DES - AES

S_6 :

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7 :

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8 :

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

μ :

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

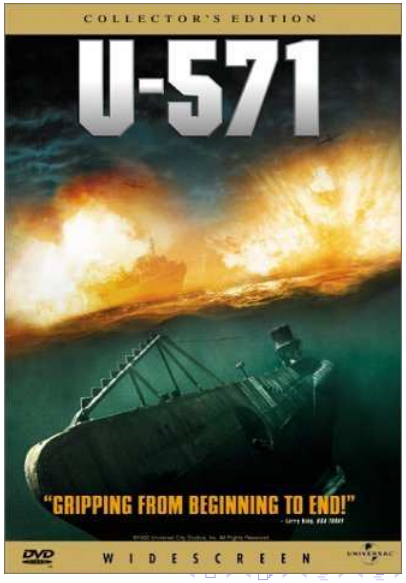
DES - AES

Depuis juin 2001, DES a été officiellement remplacé par l'AES (Advanced Encryption Standard) dont l'algorithme cryptographique *Rijndael* est d'origine belge (Joan Daemen, Vincent Rijmen)

La sélection de cet l'algorithme a été réalisée par un concours initié par le *National Institute of Standards and Technology* (NIST).

Pour palier à l'insécurité grandissante de DES, on a parfois recours à un triple DES.

Historique, la machine Enigma



FIN
de la
cryptographie
à clé secrète

MATHÉMATIQUES DISCRÈTES (5)

Michel Rigo

http://www.discmath.ulg.ac.be/

Année 2007–2008

FONCTION À SENS UNIQUE

fonction à sens unique telle que $f(x)$ est “facile” à calculer pour tout $x \in A$ et $f^{-1}(y)$ est “difficile à calculer”.

La notion de “facilité” fait référence aux ressources à mettre en oeuvre pour effectuer les calculs de f et f^{-1} (complexité temporelle).

FONCTION À SENS UNIQUE

Dumbeldore, A.	03189228
⋮	⋮
Fudge, C.	02162276
Ganger, H.	04122782
⋮	⋮
Hagrid, R.	02765100
Potter, H.	04378128
⋮	⋮

REMARQUE

Fonction à sens unique “pure” / Fonction à trappe cachée

RSA

Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman (1977)

RSA

Bob choisit deux grands nombres premiers distincts p et q.

$$n = p.q.$$

Puisque p et q sont premiers,

$$\varphi(n) = (p-1).(q-1).$$

Bob choisit à présent deux nombres e et d tels que

$$d.e \equiv 1 \mod \varphi(n).$$

Pour ce faire, il choisit e tel que

$$1 < e < \varphi(n) \quad \text{et} \quad \text{pgcd}(e, \varphi(n)) = 1.$$

Ensuite, Bob obtient d grâce à l'algorithme d'Euclide étendu.

Bob publie n, e et conserve secret les autres éléments $d, p, q, \varphi(n)$.

RSA

e (resp. d) l'*exposant de chiffrement* (resp. *de déchiffrement*). $k = (e, n)$ est la clé du système.

Si l'ensemble des textes clairs est $\mathcal{P} = \mathbb{Z}_n$, alors

$$\forall x \in \mathbb{Z}_n,\ e_k(x) := x^e \mod n.$$

PROPOSITION

Si $k = (e, n)$ et si $y = e_k(x)$, alors

$$y^d \mod n = x.$$

RSA

Petit théorème de Fermat : si $\text{pgcd}(x, n) = 1$, alors

$$x^{\varphi(n)} \equiv 1 \mod n.$$

Ici, $y = x^e$. Ainsi, il existe $\alpha \in \mathbb{N}$ tel que

$$y^d = (x^e)^d = x^{ed} = x^{1+\alpha\varphi(n)}$$

car $ed \equiv 1 \mod \varphi(n)$. Si x est premier avec n, le résultat est OK en appliquant le petit théorème de Fermat.

Supposons x non premier avec n. Il est cependant premier avec p ou q car sinon, il serait multiple de n, or $x < n$.

Supposons dès lors, x premier avec p mais pas avec q. Par le petit théorème de Fermat,

$$x^{ed} = x\,(x^{p-1})^{\alpha(q-1)} \equiv x \mod p$$

car $x^{p-1} \equiv 1 \mod p$. On a aussi trivialement

$$x^{ed} \equiv x \mod q$$

car les deux membres sont congrus à zéro modulo q.

RSA

De ces deux égalités, puisque p et q sont premiers et distincts, on en tire que

$$x^{ed} \equiv x \mod n.$$

En effet, si $y \equiv x \mod p$ et $y \equiv x \mod q$,
$y = x + m_1 p$ et $y = x + m_2 q$.
De là, $m_1 p = m_2 q$.
Puisque p et q sont premiers et distincts, $p|m_2$ et $q|m_1$.
Il existe α_1 et α_2 tels que $m_1 = \alpha_1 q$ et $m_2 = \alpha_2 p$.
De $m_1 p = m_2 q$, on tire $\alpha_1 pq = \alpha_2 pq$. D'où $\alpha_1 = \alpha_2$ et
$y = x + \alpha_1 pq = x + \alpha_1 n$.

RSA

En résumé, on a les données suivantes :

- Bob publie : $k = (e, n)$,
- Bob conserve secret : d, p, q, $\varphi(n)$,
- fonction de chiffrement : $e_k(x) = x^e \mod n$,
- fonction de déchiffrement : $d_k(y) = y^d \mod n$.

RSA

REMARQUE

Supposons qu'Alice et Bob désirent converser par courrier électronique en utilisant le RSA. Dans ce cas, Alice construit des nombres n_A, e_A, d_A et publie $k_A = (e_A, n_A)$. Bob fait de même. Il construit n_B, e_B, d_B et publie $k_B = (e_B, n_B)$. Alice (resp. Bob) utilisera alors e_{k_B} (resp. e_{k_A}) pour chiffrer des messages destinés à Bob (resp. Alice). En pratique, on peut donc supposer disposer d'une sorte d'annuaire reprenant les utilisateurs et leur clé publique respective.

RSA

EXEMPLE

$$p = 11,\ q = 23,\ n = p.q = 253,\ e = 3.$$

Puisque $220 = 3.73 + 1$, on en déduit que l'exposant de déchiffrement d est tel que

$$3^{-1} = -73 \mod 220 = 147 \mod 220.$$

Bob publie $k = (3, 253)$. Si Alice veut envoyer le texte clair $x = 165$ à Bob, elle calcule

$$e_k(x) = 165^3 \mod 253 = 110.$$

Si Bob reçoit le message $y = 110$, il lui suffit de calculer

$$d_k(y) = 110^{147} = 110^{128}.110^{16}.110^{2}.110^{1} \mod 253 = 165.$$

RSA

$p, q \sim 2^{512}$.

$$\lfloor \log_{10} 2^{512} \rfloor = \left\lfloor 512 \underbrace{\log_{10} 2}_{\sim 0,3} \right\rfloor = 154$$

REMARQUE

$N = 26, 32$ ou 256 est bien trop petit par rapport à $n \sim 2^{1024}$. Si on utilisait comme ensemble de textes clairs $\mathbb{Z}_N$ au lieu de $\mathbb{Z}_n$, alors une recherche exhaustive de toutes les images $x^e \mod n$ pour $x \in \mathbb{Z}_N$ réduit à néant la sécurité du RSA.

unité de base, les blocs de k symboles consécutifs de l'alphabet Σ avec k défini par

$$k := \left\lfloor \log_N n \right\rfloor,$$

autrement dit, $N^k \leq n < N^{k+1}$.

RSA

k éléments consécutifs de $\mathbb{Z}_N$ correspondent à un nombre $x \in \mathbb{Z}_{N^k}$ écrit en base N et compris entre 0 et $N^k - 1$.

k est la plus grande valeur possible permettant ce codage. Si $x \in \mathbb{Z}_{N^k}$, le chiffrement de x est donné par

$$y = x^e \mod n$$

qui est un entier $y < n$ et $n < N^{k+1}$.

La représentation de y en base N peut être de longueur $k + 1$. Les blocs de k éléments consécutifs de $\mathbb{Z}_N$ sont envoyés de manière injective sur des blocs de longueur $k + 1$.

RSA

EXEMPLE

$n = 253$ et $e = 3$. L'alphabet $\Sigma = \{a, b, c, d\}$ et le codage $a \to 0$, $b \to 1$, $c \to 2$, $d \to 3$). $N = \#\Sigma = 4$ donc

$$k = \left\lfloor \log_4 253 \right\rfloor = 3$$

car $4^3 = 64$ et $4^4 = 256$. Alice désire envoyer à Bob le message

bccadb

Tout d'abord, le premier bloc de longueur 3, *bcc*, correspond à

$$1.4^2 + 2.4 + 2.1 = 26 < 64$$

RSA

EXEMPLE

et son chiffrement est donné par

$$26^3 \mod 253 = 119 = 1.4^3 + 3.4^2 + 1.4^2 + 3.4^0$$

qui correspond au mot *bdbd*. Le second bloc de texte clair, *adb*, correspond à

$$0.4^2 + 3.4 + 1 = 13$$

et son chiffrement 13^3 mod $253 = 173 = 2.4^3 + 2.4^2 + 3.4^1 + 1.4^0$ fournit le mot *ccdb*.

Alice transmet le texte chiffré *bdbdccdb* Quant à Bob, il sait qu'il doit redécouper le texte chiffré en blocs de longueur $k + 1 = 4$ avant déchiffrement.

RSA

Question

Comment Bob peut-il être certain que le message provient bien d'Alice et non pas d'Oscar se faisant passer pour Alice ?

$n_A, e_A, d_A\ n_B, e_B, d_B$

Idée :

$$Alice : x \longrightarrow x^{d_A} \longrightarrow (x^{d_A})^{e_B}$$

$$Bob : (x^{d_A})^{e}_{B} \longrightarrow ((x^{d_A})^{e_B})^{d_B} = x^{d_A} \longrightarrow (x^{d_A})^{e_A} = x$$

RSA

En pratique

Si $n_A > n_B$, alors des $x^{d_A} \mod n_A$ distincts peuvent être égaux modulo n_B et le protocole proposé ne serait dès lors plus injectif.

Alice et Bob décident d'une valeur commune t.

Ils construisent chacun deux cryptosystèmes RSA

- Alice publie $(e_{A,s}, n_{A,s})$ et $(e_{A,c}, n_{A,c})$
- Bob publie $(e_{B,s}, n_{B,s})$ et $(e_{B,c}, n_{B,c})$

La construction suppose que

$$n_{A,s} < t < n_{A,c} \quad \text{et} \quad n_{B,s} < t < n_{B,c}.$$

De cette manière, Alice signe son message en utilisant l'exposant $d_{A,s}$ pour obtenir un nombre inférieur à $n_{A,s}$. Enfin, le message est chiffré avec les clé $(e_{B,c}, n_{B,c})$ et on a bien $n_{A,s} < n_{B,c}$.

RSA

Remarque

Pas raisonnable qu'Alice et Bob emploient le même n, car alors, connaissant tous deux la factorisation de n, ils pourraient déchiffrer les messages destinés à l'autre utilisateur.

Problème de signature cachée

Pour tous $x_1, x_2 \in \mathbb{Z}_n$,

$$(x_1 x_2)^d = x_1^d\, x_2^d \mod n \quad (d = d_A).$$

Si Alice signe les messages $x = x_1 x_2$ et x_2, elle signe également, sans pour autant le vouloir, le message x_1.

En effet, si on dispose de x^d et de x_2^d, on trouve

$$x_1^d = x^d (x_2^d)^{-1} \mod n$$

et ce même sans avoir connaissance de l'exposant d.

A condition que x_2^d soit inversible (très probable : $\varphi(n)/n = (p-1)(q-1)/pq$).

Construire des fonctions de hachage t.q.

$$\mu(x_1 x_2) \neq \mu(x_1)\mu(x_2)$$

et qu'il est "difficile" de trouver $x_1 \neq x_2$ t.q. $\mu(x_1) = \mu(x_2)$.

On applique la fonction de hachage μ au texte T à signer dans son intégralité et le résultat est un texte $\mu(T)$ de taille fixe (souvent 160 bits).

Uniquement le résultat est signé : $(\mu(T))^d \mod n$.

La fonction de hachage μ n'est pas injective, mais on cherche à minimiser la probabilité que deux textes distincts ayant du sens possèdent la même image par μ.

Permet aussi de diminuer le nombre de calculs à effectuer pour une signature.

But

Trouver d (resp. $\varphi(n)$) est aussi difficile que factoriser n.

Plus précisément, Si on dispose de d (resp. de $\varphi(n)$) , alors on peut construire un algorithme permettant de factoriser n.

Si d est connu

On pose

$$s = \max\{t \in \mathbb{N} \mid 2^t \text{ divise } ed-1\} \quad \text{et} \quad k = \frac{ed-1}{2^s}.$$

càd, 2^s est la plus grande puissance de 2 qui divise $ed-1$.

Lemme

Si a est premier avec n, l'ordre de a^k dans le groupe multiplicatif $\mathbb{Z}_n^*$ est de la forme 2^i pour un $i \in \{0, \ldots, s\}$.

Puisque a est premier avec n, le petit théorème de Fermat stipule que

$$a^{ed-1} \equiv 1 \mod n.$$

Par définition de k, on a $ed-1 = k2^s$ et donc

$$(a^k)^{2^s} \equiv 1 \mod n.$$

Donc l'ordre de a^k divise 2^s.

Proposition

Soit a premier avec n. Si les ordres de a^k modulo p et modulo q diffèrent, alors il existe $t \in \{0, \ldots, s-1\}$ tel que

$$1 < \text{pgcd}(a^{2^t k} - 1, n) < n.$$

Par le lemme précédent, il existe $i \leq s$ tel que

$$(a^k)^{2^i} = 1 + \alpha n = 1 + (\alpha p)q.$$

2^i est un multiple de l'ordre de a^k modulo q
$\rightarrow$ l'ordre de a^k modulo q est de la forme 2^t
$\rightarrow$ l'ordre de a^k modulo p est de la forme $2^{t'}$.

Par hypothèse, les ordres diffèrent, supp. $t < t' \leq s$. De là, on a

$$(a^k)^{2^t} \equiv 1 \mod q \quad \text{et} \quad (a^k)^{2^t} \not\equiv 1 \mod p.$$

Ainsi, $(a^k)^{2^t} - 1$ est un multiple de q mais pas de p et

$$\text{pgcd}(a^{2^t k} - 1, n) = q.$$

Algorithme (factoriser n)

Choisir aléatoirement $a \in \{1, \ldots, n-1\}$.
Calculer $g = \text{pgcd}(a, n)$.
  Si $g > 1$, on a trouvé un facteur de n.
  Si $g = 1$,
    pour $t = s-1, s-2, \ldots$
      calculer $g' = \text{pgcd}(a^{2^t k} - 1 \mod n, n)$
    jusqu'à obtenir $g' > 1$ ou arriver à $t = 0$.
  Si $g' > 1$, on a trouvé un facteur de n.
  Sinon, $t = 0$, recommencer avec un nouveau choix de a.

Question

Déterminer parmi les $\varphi(n)$ candidats "a" premiers avec n combien sont tels que a^k possède des ordres différents modulo p et q.

Résultat admis

Le nombre d'entiers $a < n$, premiers avec n et tels que a^k possède des ordres différents modulo p et q est $\geq \varphi(n)/2$.

Corollaire

La probabilité de tirer consécutivement k nombres "a" au hasard dans l'algorithme et qu'aucun de ceux-ci ne permette de factoriser n est inférieure à

$$2^{-k}.$$

Si $k = 10$, $1 - 2^{-k} = 1023/1024 \sim 0,999$.

Si $\varphi(n)$ est connu

$$n = p.q \quad \text{et} \quad \varphi(n) = (p-1)(q-1).$$

En remplaçant q par n/p dans la seconde équation, on obtient

$$\varphi(n) = (p-1)(\frac{n}{p} - 1)$$

c'est-à-dire,

$$p^2 + p\,[\varphi(n) - n - 1] + n = 0.$$

Puisque $\varphi(n)$ est connu, il s'agit d'une simple équation du second degré permettant de retrouver p.

Rapidité du RSA

Si $e \simeq n = p.q$ et si l'on suppose que son écriture binaire contient autant de bits 0 que de 1, alors travaillant avec un entier $n \sim 2^{1024}$, pour réaliser une exponentiation modulaire, on a besoin de 1024 élévations au carré et 512 multiplications modulo n.

On peut estimer le RSA de 1000 à 10000 fois plus lent que le DES.

RSA pour échanger en toute sécurité une clé d'un cryptosystème à clé secrète.

QUELQUES ÉLÉMENTS DE SÉCURITÉ

1. p et q ne doivent pas être “petits”, ni provenir d’une table.

Recherche exhaustive ou tester les nombres de la table

EXEMPLE

Sous Mathematica , tester si 15485863 est divisible par l’un des cent mille premiers nombres premiers prend sur un pentium III à 600 Mhz un peu moins de $3,4$ secondes.

2. p et q ne doivent pas être trop proches.

si $p > q$, alors $(p-q)/2$ est petit et $(p+q)/2$ est un peu plus grand que $\sqrt{n}$. Par ailleurs, il est clair que

$$\left(\frac{p+q}{2}\right)^2 - n = \left(\frac{p-q}{2}\right)^2.$$

Ainsi, il suffit de considérer successivement tous les entiers $x > \sqrt{n}$ et pour ceux-ci, de calculer $x^2 - n$ jusqu’à obtenir un carré parfait y^2. Dans ce cas, $x^2 - y^2 = n$ et on trouve $p = x + y$ et $q = x - y$.

EXEMPLE, $n = 97343$

On a $\sqrt{n} > 311$ et $312^2 - n = 1$. Par conséquent, $n = 311.313$.

EXEMPLE, $n = 239812789091371$

On a $\sqrt{n} > 15485889$ et

$$15485890^2 - 239812789091371 = 729 = 27^2.$$

Donc,

$$239812789091371 = (15485890 + 27)(15485890 - 27).$$

Il s’agit en fait du produit des millionième et $(10^6 + 2)$-ième nombres premiers.

3. $p - 1$ et $q - 1$ ne doivent pas avoir un large facteur commun (i.e., un pgcd trop grand).

Sinon $u = \text{ppcm}(p-1)(q-1)$ est “relativement” petit en comparaison de $\varphi(n)$.

Tout inverse de e modulo u peut être utilisé comme exposant de déchiffrement.

En effet, si $z.e \equiv 1 \mod u$, alors $z.e = 1 + \alpha(p-1) = 1 + \beta(q-1)$ et il suffit d’adapter la seconde partie de la preuve... (déchiffrement RSA)

Bien que u soit inconnu, il peut être suffisamment petit pour procéder à une recherche exhaustive. Ainsi, il suffit de tester des candidats u successifs et pour chacun d’entre eux calculer l’inverse de e modulo u.

si $z.e \equiv 1 \mod u$, $z.e = 1 + \alpha(p-1) = 1 + \beta(q-1)$.

Soit $x \in \mathbb{Z}_n$. On a

$$(x^e)^z = x^{ez} = x(x^\alpha)^{p-1}.$$

Si x est premier avec p, alors x^α aussi et

$$x.(x^\alpha)^{p-1} \equiv x.1 \mod p.$$

Si x est un multiple de p, les deux membres ci-dessus sont congrus à 0 modulo p.
Pour tout $x \in \mathbb{Z}_n$, $(x^e)^z \equiv x$ modulo p.

raisonnement idem pour q. On en tire que pour tout $x \in \mathbb{Z}_n$, $(x^e)^z \equiv x$ modulo n, z est bien un exposant de déchiffrement.

EXEMPLE

Soient $p = 61$, $q = 181$, $n = 11041$ et $e = 4013$. Ici, $\varphi(n) = 60.180 = 10800$. Ici, $\text{ppcm}(p-1, q-1) = q - 1$.

Le ppcm étant pair, il suffit de tester successivement pour candidats $u = 2, 4, \ldots, 180$.

Après 90 tests, Oscar est en mesure de construire un exposant de déchiffrement.

EXEMPLE

Soient $p = 61$, $q = 179$, $n = 10919$ et $e = 4013$. Ici, $\varphi(n) = 60.178 = 10680$. Du point de vue de l'ordre de grandeur, les différences sont minimes. Néanmoins, ici

$$\text{ppcm}(60, 178) = 60.89 = 5340$$

la recherche exhaustive nécéssite 2770 essais.

4. Si $\varphi(n)$ ne possède que de petits facteurs premiers, i.e.,

$$\varphi(n) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad p_i \leq r$$

où r est une borne suffisamment petite ($p_1, \ldots, p_k$ représentent tous les nombres premiers $\leq r$ et $\alpha_i = 0$ si p_i n'apparaît pas).

$$p_i^{\lfloor \log_{p_i} n \rfloor}$$

est la plus grande puissance de p_i qui peut éventuellement diviser $\varphi(n)$ (en effet, $\varphi(n) < n$ et ne connaissant pas la valeur de $\varphi(n)$, on utilise alors n comme estimation).

On décide de passer en revue les candidats potentiels pour $\varphi(n)$: ils sont de la forme

$$u = p_1^{\beta_1} \cdots p_k^{\beta_k} \text{ avec } \beta_i \leq \lfloor \log_{p_i} n \rfloor, \forall i \leq k.$$

Pour chaque candidat potentiel u :
si $(u+1)/e$ est un entier d', on essaye d' comme exposant de déchiffrement (c'est assez naturel, car alors $ed' = 1 + u$).

Si r n'est pas trop grand, les candidats potentiels à tester ne sont pas trop nombreux et une recherche exhaustive est réalisable.

Exemple

Soit n le produit des 100- et 101-ièmes nombres premiers,

$$n = 295927 \text{ et } \varphi(n) = 2^3.3^4.5.7.11^0.13$$

et $\log_2 n = 18$, $\log_3 n = 11$, $\log_5 n = 7$, $\log_7 n = 6$, $\log_{11} n = 5$, $\log_{13} n = 4$.

Les candidats u sont (en considérant $r = 13$) de la forme

$$2^{i_1}.3^{i_2}.5^{i_3}.7^{i_4}.11^{i_5}.13^{i_6}$$

avec $0 \leq i_1 \leq 18$, $0 \leq i_2 \leq 11$, $0 \leq i_3 \leq 7$, $0 \leq i_4 \leq 6$, $0 \leq i_5 \leq 5$ et $0 \leq i_6 \leq 4$. Le nombre total de candidats est donc

$$19.12.8.7.6.5 = 383040.$$

Exemple

Par contre, pour n, produit des 101- et 102-ièmes nombres premiers, on a

$$n = 304679 \text{ et } \varphi(n) = 2^3.3.7.13.139.$$

Ici, le plus grand facteur premier apparaissant dans la décomposition de $\varphi(n)$ est 139 (qui est le 34-ième nombre premier) et si on procède comme ci-dessus, les candidats u sont de la forme

$$2^{i_1}.3^{i_2}.5^{i_3}.7^{i_4} \cdots 131^{i_{32}}.137^{i_{33}}.139^{i_{34}}$$

et le nombre total de candidats est

$$5149048008867840.$$

5. Si les exposants e et d sont petits, il existe également des attaques possibles du RSA.

Compromis entre sécurité et temps de calcul (par exemple, pour un système RSA placé sur une carte à puce pour laquelle les ressources de calcul sont limitées)

Génération de grandes nombres premiers

Trouver un nombre premier de k bits écrit en base 2, on considère un vecteur appartenant à $\{0,1\}^k$: $1 * \cdots * 1$.

Tests de primalité

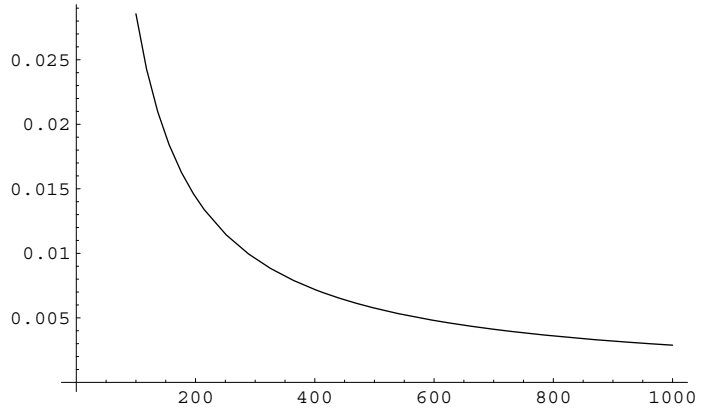
Approximation du nombre de tirages à réaliser pour obtenir un nombre premier de k bits

le nombre de nombres premiers de k bits est

$$\pi(2^k) - \pi(2^{k-1}) \sim \frac{2^k}{\ln 2^k} - \frac{2^{k-1}}{\ln 2^{k-1}}$$

et le nombre total d'entiers impairs de k bits est 2^{k-2}.

$k = 100$, proba proche de $0,0285$ et pour $k = 512$, $0,0056$.



La réponse est : soit “*m* est composé” (on ne dispose pas de la factorisation de *m* mais on est certain que ce nombre n’est pas premier)
soit “*m* est peut-être premier”. En effet, pour *m* composé, il existe des entiers *x* tels que $x^{m-1} \equiv 1 \mod m$. La détermination du caractère composé de *m* dépend de l’entier *x* tiré aléatoirement.

Le petit théorème de Fermat fournit un test de primalité probabiliste.

Si *m* est premier, alors $x^{m-1} \equiv 1 \mod m$. Donc, si pour *x* premier avec *m*, on a $x^{m-1} \not\equiv 1 \mod m$, alors on en conclut directement que *m* n’est pas premier.

TEST DE PRIMALITÉ DE FERMAT, DONNÉE *m*

Choisir aléatoirement *x* tel que $1 \leq x < m$.
Calculer $g = \text{pgcd}(x, m)$.
  Si $g > 1$, alors *m* n’est pas premier.
  Sinon, calculer $t = x^{m-1} \mod m$.
    Si $t \not\equiv 1$, alors *m* est composé.
    Si $t \equiv 1$, alors *m* est peut-être premier.

EXEMPLE

Si *x* est tq. $1 \leq x < m$, $\text{pgcd}(x, m) = 1$ et $x^{m-1} \equiv 1 \mod m$, alors *x* est témoin de la primalité de *m* ou
m est un nombre pseudo-premier relativement à la base *x*.

“Au plus on a de témoins, au plus on y croît !”

EXEMPLE

Le nombre 91 est composé, $91 = 13.7$.

$$2^{90} = 2^{64}.2^{16}.2^{8}.2^{2} \equiv 64 \mod 91.$$

Ainsi, si on tire aléatoirement $x = 2$, on montre que 91 n’est pas premier : “2 n’est pas témoin de la primalité de 91”.

Par contre, $3^{90} = 3^{64}.3^{16}.3^{8}.3^{2} \equiv 1 \mod 91$.

Dès lors, si on tire $x = 3$, on n’est pas en mesure de prouver la non primalité de 91 : “91 est pseudo-premier relativement à 3”.

PROPOSITION

Considérons un entier m. Soit tous, soit au plus la moitié des entiers x tels que $1 \leq x < m$ et $\text{pgcd}(x, m) = 1$ sont témoins de la primalité de m.

REMARQUE

Dans la situation où un entier composé m est tel qu'au plus la moitié des entiers x sont témoins de la primalité de m, si on effectue k tests consécutifs, la probabilité que m soit considéré comme pseudo-premier à l'issue de ces k tests est $\leq 2^{-k}$.

DÉFINITION

Il existe des nombres composés m pour lesquels tout $x < m$ et premier avec m est témoin de primalité de m, i.e., $x^{m-1} \equiv 1 \mod m$. Un tel nombre est appelé nombre de Carmichael.

Test de Fermat :-(

Le seul espoir bien faible de détecter la non primalité d'un tel nombre m est de tirer au hasard un nombre x ayant un facteur commun avec m.

Supposons que x n'est pas témoin de la primalité de m, i.e.,

$$x^{m-1} \not\equiv 1 \mod m.$$

Soient $w_1, \ldots, w_t$ tous les témoins (distincts) de primalité de m. Posons

$$u_i = x\, w_i \mod m.$$

Les u_i sont tous distincts car x est premier avec m donc inversible modulo m. Si $u_i = u_j$ avec $i \neq j$, alors on en déduirait que $w_i = w_j$, ce qui est impossible. De plus, $1 \leq u_i < m$ et $\text{pgcd}(u_i, m) = 1$ car x et les w_i, par définition, sont premiers avec m. Les u_i ne sont pas témoins de la primalité de m. En effet,

$$u_i^{m-1} = \underbrace{x^{m-1}}_{\not\equiv 1} \underbrace{w_i^{m-1}}_{\equiv 1} \not\equiv 1 \mod m.$$

Conclusion : s'il existe x non témoin de la primalité de m, alors il y a au moins autant de nombres u_i non témoins que de w_i qui sont témoins.

PROPOSITION

Un nombre composé m est de Carmichael SSI il n'est divisible par aucun carré (square-free ou quadratfrei) et pour tout p premier divisant m, $p - 1$ divise $m - 1$.

EXEMPLE

Le nombre $561 = 3.11.17$ est un nombre de Carmichael (c'est même le plus petit). En effet, $560 = 280.2$, $560 = 56.10$ et $560 = 35.16$.

On pourrait vérifier que tout $x < m$ et premier avec m est tel que $x^{m-1} \equiv 1 \mod m$.

$\Rightarrow$ Soit $m \geq 3$ un nombre de Carmichael.
Soit p un diviseur premier de m.
Soit a racine primitive modulo p (i.e., un générateur de $\mathbb{Z}_p^*$) qui est premier avec m. Un tel a existe.

$\mathbb{Z}_p$ est un champ, $\mathbb{Z}_p^*$ possède $\varphi(p-1)$ générateurs. Soit u un de ces générateurs modulo p.
Si $m = p^\alpha q_1^{\beta_1} \cdots q_r^{\beta_r}$, alors a s'obtient par exemple comme solution du système

$$\begin{cases} a \equiv u \mod p, \\ a \equiv 1 \mod q_1, \\ \vdots \\ a \equiv 1 \mod q_r. \end{cases}$$

Si a est solution de ce système, il est nécessairement premier avec m puisqu'il n'a aucun facteur commun avec m. Le théorème des restes chinois assure l'existence d'un tel a.

Théorème des restes chinois

Si $m_1, \ldots, m_n$ sont deux à deux premiers, le système

$$x \equiv a_1 \mod m_1, \ldots, x \equiv a_n \mod m_n$$

possède une unique solution modulo $m = m_1 \cdots m_n$. Si, pour tout $i = 1, \ldots, n$, on pose $M_i = m/m_i$ et $y_i = M_i^{-1} \mod m_i$, alors cette solution est donnée par

$$x = \left(\sum_{i=1}^{n} a_i y_i M_i \right) \mod m.$$

Puisque a est premier avec m (nombre de Carmichael), on a $a^{m-1} \equiv 1 \mod m$ et donc $a^{m-1} \equiv 1 \mod p$ (car $p|m$).
a racine primitive mod p, son ordre modulo p est $p-1$ donc $p-1$ divise $m-1$.

p^2 ne divise pas m ? P.A. Supposons que p^2 divise m.

$\varphi(m)$ est divisible par $p(p-1)$ et en particulier par p.
Dès lors, $\mathbb{Z}_m^*$ qui est un groupe contenant $\varphi(m)$ éléments contient un sous-groupe d'ordre p et donc aussi un élément $b \in \mathbb{Z}_m^*$ premier avec m et d'ordre p modulo m.

Lemme de Cauchy

Tout groupe commutatif fini dont l'ordre est divisible par un nombre premier p contient un élément d'ordre p.
Dans le cas général, conséquence du premier théorème de Sylow : tout groupe fini dont l'ordre est divisible par un nombre premier p contient un élément d'ordre p.

Puisque m est de Carmichael, $b^{m-1} \equiv 1 \mod m$ donc p doit diviser $m-1$.

Impossible car p divise m.

$\Leftarrow$ Supposons m est sans carré et $p-1$ divise $m-1$ pour tout facteur premier p de m.

Soient a premier avec m et p un diviseur premier de m.

Thèse : $a^{m-1} \equiv 1 \mod m$.

petit théorème de Fermat : $a^{p-1} \equiv 1 \mod p$.
Puisque $m-1$ est un multiple de $p-1$, : $a^{m-1} \equiv 1 \mod p$.
Cette congruence est OK pour tout diviseur premier de m.

Or $m = p_1 \cdots p_r$ (avec $p_i \neq p_j$, si $i \neq j$ car m est sans carré), alors pour tout $i = 1, \ldots, r$, $a^{m-1} \equiv 1 \mod p_i$.
De là, on en tire que

$$a^{m-1} \equiv 1 \mod m.$$

Corollaire

Un nombre m de Carmichael est toujours impair.

Si $p \geq 3$ est un facteur premier de m, $p-1$ divise $m-1$.
Or $p-1$ est pair donc $m-1$ l'est aussi.

Remarque

Il existe une infinité de nombres de Carmichael :
W. R. Alford, A. Granville, C. Pomerance, There Are Infinitely Many Carmichael Numbers, Ann. Math. **139**, *703–722, (1994)*.

Le nombre de nombres de Carmichael inférieurs à 10^{17} est 585355 à comparer avec $\pi(10^{17}) \sim 2,5.10^{15}$.

Pour la fonction comptant le nombre de nombres de Carmichael $\leq n$, pas de résultats analogues à $\pi(n)$. Recourir à des techniques de calcul élaborées pour les énumérer :
R.G.E. Pinch, The Carmichael numbers up to 10^{15}*, Mathematics of Computation* **61**, *381–391 (1993).*

Proposition

Si $m \geq 3$ est impair, il y a au plus $(m-1)/4$ entiers $x < m$ premiers avec m et non témoins du caractère composé de m.

Corollaire

Si on applique k fois consécutivement le test de Miller-Rabin à un nombre composé m, la probabilité de ne pas découvrir son caractère composé est inférieure à 4^{-k}.

Test de Miller-Rabin

Soit $m > 1$ un nombre impair. On pose

$$s = \max\{r \in \mathbb{N} \mid 2^r \text{ divise } m-1\} \quad \text{et} \quad d = \frac{m-1}{2^s}.$$

Théorème (admis) "à la Fermat"

Si m est un nombre premier et si $x \in \mathbb{Z}$ est premier avec m, alors l'une des deux conditions est satisfaite :

- $x^d \equiv 1 \mod m$,
- il existe $r \in \{1, \ldots, s-1\}$ tel que $x^{2^r d} \equiv -1 \mod m$.

$\Rightarrow$ Algorithme pour tester la primalité d'un entier m.

Si un entier x premier avec m est tel que aucune des deux conditions du thm n'est satisfaite, alors m est composé.

x est témoin du caractère composé de m. Sinon m est un nombre pseudo-premier fort (strong pseudoprime) pour la base x.

Exemple

$m = 561$ est un nombre de Carmichael. Si on applique le test de Miller-Rabin, on peut choisir $x = 2$. La plus grande puissance de 2 qui divise 560 est $16 = 2^4$ (car $560 = 16.35$). Ainsi, $s = 4$ et $d = 560/16 = 35$. On calcule

$$x^d = 2^{35} \mod 561 = 263.$$

Puisque le résultat n'est pas 1, on calcule $x^{2^r d}$ pour $r = 1, 2, \ldots, s-1$:

$2^{2.35} \mod 561 = 166$, $2^{4.35} \mod 561 = 67$, $2^{8.35} \mod 561 = 1$.

Par conséquent, aucune congruence ne donnant -1, on en déduit que 561 est composé et 2 en est le témoin.

Hypothèse de Riemann

Tous les zéros complexes de la fonction

$$\zeta : \mathbb{C} \to \mathbb{C} : s \mapsto \sum_{n=1}^{\infty} \frac{1}{n^s}$$

dont la partie réelle se trouve entre 0 et 1 ont leur partie réelle exactement égale à $1/2$. Par exemple, il est facile de voir que si $\operatorname{Re} s > 1$, alors $\zeta(s) \neq 0$ et que si $\operatorname{Re} s < 0$, alors les seuls zéros de la fonction ζ sont $-2, -4, -6, \ldots$ (appelés zéros triviaux). L'hypothèse de Riemann généralisée est du même type mais pour une généralisation de la fonction ζ, à savoir les L-séries de Dirichlet.

Agrawal *et al.* (2002)

Algorithme polynomial permettant de tester la primalité d'un entier. `Primes` $\in P$

On peut montrer, en supposant l'hypothèse de Riemann généralisée vérifiée, que si m est composé, alors il existe toujours un témoin x du caractère composé de m tel que

$$x < 2(\ln m)^2.$$

Ceci permet donc d'utiliser le test de Miller-Rabin de manière déterministe en testant tous les x jusqu'à cette borne.

RSA et nombres composés

RSA dans le cas où p et q ne sont pas nécessairement premiers. On suppose ici que

$$p = p_1 p_2 \quad \text{et} \quad p_1, p_2, q \text{premiers}.$$

On a $n = p.q = p_1.p_2.q$ et $\varphi(n) = (p_1 - 1)(p_2 - 1)(q - 1)$ Par contre, ne sachant pas que p n'est pas premier, la valeur de $\varphi(n)$ effectivement calculée est $\varphi'(n) = (p - 1)(q - 1)$. Soit

$$u = \operatorname{ppcm}(p_1 - 1, p_2 - 1, q - 1).$$

Supposons que le texte clair x est premier avec n.

Par conséquent, x est premier avec p_1, p_2, q et

$$x^{p_1-1} \equiv 1 \mod p_1,\ x^{p_2-1} \equiv 1 \mod p_2,\ x^{q-1} \equiv 1 \mod q.$$

Puisque u est multiple de $p_1 - 1$, de $p_2 - 1$ et de $q - 1$, on a aussi

$$x^u \equiv 1 \mod p_1,\ x^u \equiv 1 \mod p_2,\ x^u \equiv 1 \mod q.$$

De là, p_1, p_2, q étant premiers et distincts, on en tire

$$x^u \equiv 1 \mod n.$$

Il est clair que u divise $\varphi(n)$.

Deux situations à envisager :

- soit u divise le $\varphi'(n)$ erroné,
- ou bien u ne divise pas le $\varphi'(n)$ erroné.

- Dans le premier cas, $\alpha\, u = \varphi'(n)$ et donc

$$x^{1+k\,\varphi'(n)} = x^{1+k\,\alpha\,u} \equiv x \mod n.$$

  Par conséquent, toute paire (e, d) d'exposants de chiffrement et de déchiffrement telle que $e.d \equiv 1 \mod \varphi'(n)$ convient. (En effet, les exposants ont été calculés avec le $\varphi'(n)$ erroné.)

- Dans le second cas, les choses ne se passent pas aussi bien. En général, $d_k(e_k(x)) \neq x$! Ceci est vérifié sur l'exemple suivant.

Illustration

Soient

$$p = 391 (= 17.23) \text{ et } q = 281.$$

Ici, $n = 109871$ et le $\varphi'(n)$ calculé $= 390.280 = 109200$.

$u = \text{ppcm}\,(16 = 2^4, 22 = 2.11, 280 = 2^3.5.7) = 2^4.5.7.11 = 6160$.

Ici, u ne divise pas $\varphi'(n) = 109200 = 17.6160 + 4480$.

$e = 19$, on obtient l'inverse de e modulo $\varphi'(n)$, $d = 45979$.

Le texte clair $x = 8$ est bien premier avec n.
Nous devrions avoir $x^{ed} \equiv x \mod n$, mais

$$x^{ed} \mod 109871 = 95548 \neq 8.$$

Algorithmes de factorisation

- le crible d'Eratostène,
- le crible quadratique (quadratic sieve),
- des algorithmes sur les courbes elliptiques,
- le crible algébrique (number field sieve),
- l'algorithme ρ,
- la méthode $p - 1$ de Pollard,
- la méthode $p + 1$ de Williams,
- l'algorithme de factorisation par fractions continues,...

Le crible d'Eratostène

2	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

Le crible d'Eratostène

(2)	12	22	32	42	52
3	13	23	33	43	53
4	14	24	34	44	54
5	15	25	35	45	55
6	16	26	36	46	56
7	17	27	37	47	57
8	18	28	38	48	58
9	19	29	39	49	59
10	20	30	40	50	60
11	21	31	41	51	61

Le crible d'Eratostène

(2)	~~12~~	~~22~~	~~32~~	~~42~~	~~52~~
3	13	23	33	43	53
~~4~~	~~14~~	~~24~~	~~34~~	~~44~~	~~54~~
5	15	25	35	45	55
~~6~~	~~16~~	~~26~~	~~36~~	~~46~~	~~56~~
7	17	27	37	47	57
~~8~~	~~18~~	~~28~~	~~38~~	~~48~~	~~58~~
9	19	29	39	49	59
~~10~~	~~20~~	~~30~~	~~40~~	~~50~~	~~60~~
11	21	31	41	51	61

Le crible d'Eratostène

(2)	~~12~~	~~22~~	~~32~~	~~42~~	~~52~~
(3)	13	23	33	43	53
~~4~~	~~14~~	~~24~~	~~34~~	~~44~~	~~54~~
5	15	25	35	45	55
~~6~~	~~16~~	~~26~~	~~36~~	~~46~~	~~56~~
7	17	27	37	47	57
~~8~~	~~18~~	~~28~~	~~38~~	~~48~~	~~58~~
9	19	29	39	49	59
~~10~~	~~20~~	~~30~~	~~40~~	~~50~~	~~60~~
11	21	31	41	51	61

Le crible d'Eratostène

(2)	~~12~~	~~22~~	~~32~~	~~42~~	~~52~~
(3)	13	23	~~33~~	43	53
~~4~~	~~14~~	~~24~~	~~34~~	~~44~~	~~54~~
5	~~15~~	25	35	~~45~~	55
~~6~~	~~16~~	~~26~~	~~36~~	~~46~~	~~56~~
7	17	~~27~~	37	47	~~57~~
~~8~~	~~18~~	~~28~~	~~38~~	~~48~~	~~58~~
~~9~~	19	29	~~39~~	49	59
~~10~~	~~20~~	~~30~~	~~40~~	~~50~~	~~60~~
11	~~21~~	31	41	~~51~~	61

Le crible d'Eratostène

(2)	~~12~~	~~22~~	~~32~~	~~42~~	~~52~~
(3)	13	23	~~33~~	43	53
~~4~~	~~14~~	~~24~~	~~34~~	~~44~~	~~54~~
(5)	~~15~~	25	35	~~45~~	55
~~6~~	~~16~~	~~26~~	~~36~~	~~46~~	~~56~~
7	17	~~27~~	37	47	~~57~~
~~8~~	~~18~~	~~28~~	~~38~~	~~48~~	~~58~~
~~9~~	19	29	~~39~~	49	59
~~10~~	~~20~~	~~30~~	~~40~~	~~50~~	~~60~~
11	~~21~~	31	41	~~51~~	61

Le crible d'Eratostène

(2)	~~12~~	~~22~~	~~32~~	~~42~~	~~52~~
(3)	13	23	~~33~~	43	53
~~4~~	~~14~~	~~24~~	~~34~~	~~44~~	~~54~~
(5)	~~15~~	~~25~~	~~35~~	~~45~~	~~55~~
~~6~~	~~16~~	~~26~~	~~36~~	~~46~~	~~56~~
7	17	~~27~~	37	47	~~57~~
~~8~~	~~18~~	~~28~~	~~38~~	~~48~~	~~58~~
~~9~~	19	29	~~39~~	49	59
~~10~~	~~20~~	~~30~~	~~40~~	~~50~~	~~60~~
11	~~21~~	31	41	~~51~~	61

Le crible d'Eratostène

(2)	~~12~~	~~22~~	~~32~~	~~42~~	~~52~~
(3)	13	23	~~33~~	43	53
~~4~~	~~14~~	~~24~~	~~34~~	~~44~~	~~54~~
(5)	~~15~~	~~25~~	~~35~~	~~45~~	~~55~~
~~6~~	~~16~~	~~26~~	~~36~~	~~46~~	~~56~~
(7)	17	~~27~~	37	47	~~57~~
~~8~~	~~18~~	~~28~~	~~38~~	~~48~~	~~58~~
~~9~~	19	29	~~39~~	49	59
~~10~~	~~20~~	~~30~~	~~40~~	~~50~~	~~60~~
11	~~21~~	31	41	~~51~~	61

Le crible d'Eratostène

2	~~12~~	~~22~~	~~32~~	~~42~~	~~52~~
3	13	23	~~33~~	43	53
~~4~~	~~14~~	~~24~~	~~34~~	~~44~~	~~54~~
5	~~15~~	~~25~~	~~35~~	~~45~~	~~55~~
~~6~~	~~16~~	~~26~~	~~36~~	~~46~~	~~56~~
7	17	~~27~~	37	47	~~57~~
~~8~~	~~18~~	~~28~~	~~38~~	~~48~~	~~58~~
~~9~~	19	29	~~39~~	~~49~~	59
~~10~~	~~20~~	~~30~~	~~40~~	~~50~~	~~60~~
11	~~21~~	31	41	~~51~~	61

Le crible d'Eratostène

2	~~12~~	~~22~~	~~32~~	~~42~~	~~52~~
3	13	23	~~33~~	43	53
~~4~~	~~14~~	~~24~~	~~34~~	~~44~~	~~54~~
5	~~15~~	~~25~~	~~35~~	~~45~~	~~55~~
~~6~~	~~16~~	~~26~~	~~36~~	~~46~~	~~56~~
7	17	~~27~~	37	47	~~57~~
~~8~~	~~18~~	~~28~~	~~38~~	~~48~~	~~58~~
~~9~~	19	29	~~39~~	~~49~~	59
~~10~~	~~20~~	~~30~~	~~40~~	~~50~~	~~60~~
11	~~21~~	31	41	~~51~~	61

Le crible d'Eratostène

Imaginons un ordinateur capable de réaliser 10^9 divisions par seconde ! Si n est de l'ordre de 2^{1024}, $\sqrt{n} \sim 10^{150}$. Il faudrait donc au crible d'Eratostème près de 10^{140} secondes ce qui dépasse de très loin l'âge de l'univers !

Méthode $p-1$ de Pollard (1974)

Factoriser n et on se fixe une borne B

Algorithme de Pollard

Choisir aléatoirement $g \in \{2, \ldots, n-1\}$.
Calculer $t = \mathrm{pgcd}(g, n)$.
  Si $t > 1$, alors on a trouvé un facteur de n.
  Sinon, calculer $a = g^{B!} \mod n$.
  Calucler $d = \mathrm{pgcd}(a-1, n)$.
    Si $d > 1$, d est un facteur.
    Sinon, facteur non trouvé, recommencer avec $B >$.

Soit p un facteur premier de n tq toute puissance r^α d'un nombre premier r, divisant $p-1$, soit $\leq B$.

$$p-1 = r_1^{\alpha_1} \cdots r_t^{\alpha_t} \text{ avec } r_i^{\alpha_i} \leq B,\ \forall i.$$

Si B est "suffisamment petit", il est facile de déterminer un multiple de $p-1$ sans pour autant connaître de $p-1$.

Puisque $a \equiv g^{B!} \mod n$, on a $a \equiv g^{B!} \mod p$ car $p|n$. Par le petit théorème de Fermat : $g^{p-1} \equiv 1 \mod p$
(si g est premier avec p, ce que nous supposons vu l'algorithme).

Puisque tout facteur r^α de $p-1$ est $\leq B$, on a

$$p-1 \text{ divise } B!$$

car $r_i \neq r_j$ et chaque $r_i^{\alpha_i} \leq B$.

De là,

$$a \equiv g^{B!} = g^{m(p-1)} = (g^{p-1})^m \equiv 1 \mod p$$

et $a-1$ est un multiple de p. Par conséquent, il ne reste plus qu'à calculer le pgcd de n et de $a-1$.

On retrouve donc d'une certaine façon la mise en garde **3.** concernant le choix de p et q dans l'élaboration du RSA.

Illustration

Considérons l'entier (composé) $n = 15770708441$.
Avec $g = 2$ et B fixé à 200, on calcule

$$g^{200!} \mod n = 6094850739.$$

Ensuite, on calcule le pgcd de $6094850739 - 1$ et de n et on trouve

$$135979$$

qui est donc un facteur de n.

Illustration

En fait, n est le produit des deux nombres premiers suivants :

$$p = 115979\ (p-1 = 2.103.563)$$

$$q = 135979\ (q-1 = 2.3.131.173).$$

Une borne $B \geq 173$ permettra la factorisation de n.

On pourra observer qu'une borne $B \geq 563$ ne donnera plus de résultat, car dans ce cas, a sera congru à 1 modulo p et q donc aussi modulo n. De toute façon, en pratique, on considère les bornes les plus petites possibles.

REMARQUE

Cet algorithme fonctionne en un temps polynomial en n à condition que la borne convenanble B soit en $\mathcal{O}((\log n)^i)$.

Cependant, pour un grand nombre n arbitraire, il est probable que la borne B doive augmenter jusque $\sqrt{n}$ et dans ce cas, la méthode $p-1$ n'est pas plus rapide que le crible d'Eratostène.

- 1998, des nombres $\sim 10^{70}$ pouvaient être factorisés en 10 heures sur une station de travail.
- A cette même époque, il fallait un an pour factoriser un nombre de 100 chiffres décimaux sur une station.
- 1999, un nombre de 155 chiffres a été factorisé en plus de 5 mois par 292 ordinateurs en réseau. Des calculs préalables à la factorisation ont pris près de 4 mois à des super-ordinateurs CRAY.
- Décembre 2003, le "RSA Challenge number" `RSA-576` de 576 bits (174 chiffres décimaux) a été factorisé `http ://www.rsasecurity.com/`

- Le "RSA Challenge number" `RSA-640` de 640 bits suivant

  3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

  factorisé le 5 novembre 2005 (193 chiffres décimaux), 20000$. 4 mois de calculs en réseau, représente plus de 30 ans de calcul pour un seul processeur Opteron cadencé à 2,2 Ghz.
- A titre indicatif, on propose 100000$ pour le challenge number `RSA-1024` ...

- Le "RSA Challenge number" `RSA-640` de 640 bits suivant

  3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609

  factorisé le 5 novembre 2005 (193 chiffres décimaux), 20000$. 4 mois de calculs en réseau, représente plus de 30 ans de calcul pour un seul processeur Opteron cadencé à 2,2 Ghz.
- A titre indicatif, on propose 100000$ pour le challenge number `RSA-1024` ...

Let us quote

"*Using a minimal key length of* 1024 *bits, it is guaranteed that RSA can be considered safe for the near future as long as there will be no fundamental advance in the factoring of large numbers.*"

Let us quote

"*Clearly, the factoring of a challenge-number of specific length does not mean that the RSA cryptosystem is "broken." It does not even mean, necessarily, that keys of the same length as the factored challenge number must be discarded. It simply gives us an idea of the amount of work required to factor a modulus of a given size. This can be translated into an estimate of the cost of breaking a particular RSA key pair.*

Suppose, for example, that in the year 2010 a factorization of RSA-768 is announced that requires 6 months of effort on 100,000 workstations. In this hypothetical situation, would all 768-bit RSA keys need to be replaced ? The answer is no. If the data being protected needs security for significantly less than six months, and its value is considerably less than the cost of running 100,000 workstations for that period, then 768-bit keys may continue to be used."

Logarithme discret

Soit G un groupe multiplicatif cyclique contenant n éléments et γ un générateur de G.

Définition

Soit $x \in G$. Le logarithme discret de x est le plus petit d tq

$$x = \gamma^d.$$

$\mathrm{dlog}_\gamma : G \to \{1, \ldots, |G|\}$, $\mathrm{dlog}\, x = d$ ou $\mathrm{dlog}_\gamma\, x = d$

Exemple

Dans $\mathbb{Z}_{17}^*$, 3 est générateur,

i	1	2	3	4	5	6	7	8	9	10	11	12	13	$\cdots$
3^i	3	9	10	13	5	15	11	16	14	8	7	4	12	$\cdots$

$$\mathrm{dlog}_3\, 15 = 6 \text{ et } \mathrm{dlog}_3\, 14 = 9.$$

Fonction à sens unique

Si $G = \mathbb{Z}_p^*$ où p est un grand nombre premier, alors $\mathbb{Z}_p^*$ est cyclique. Si on se donne un générateur γ et un élément $x \in \mathbb{Z}_p^*$, le calcul du logarithme discret est conjecturé être difficile.

Par contre, exponentiation (modulaire) est "facile".

- l'algorithme "baby-step giant-step" de Shanks,
- la ρ-méthode de Pollard,
- l'algorithme de Pohlig-Hellman,
- le calcul d'indices,...

Aucun algorithme connu à ce jour ne donne de résultats satisfaisant pour des nombres premiers p arbitraires suffisamment grands.

Les complexités des algorithmes de factorisation de grands nombres et de recherche de logarithme discret sont proches.

Remarque

Si $G = (\mathbb{Z}_p^*, \cdot)$, alors $\mathbb{Z}_p^*$ est cyclique d'ordre $p-1$ donc isomorphe au groupe additif $(\mathbb{Z}_{p-1}, +)$. Il existe une bijection

$$\psi : (\mathbb{Z}_p^*, \cdot) \to (\mathbb{Z}_{p-1}, +)$$

tq. $\psi(xy \mod p) = \psi(x) + \psi(y) \mod p-1$.
On en tire que $\psi(\gamma^a \mod p) = a\,\psi(\gamma) \mod p-1$. Donc

$$\begin{aligned} x \equiv \gamma^a \mod p &\Leftrightarrow \psi(x) \equiv a\,\psi(\gamma) \mod p-1 \\ &\Leftrightarrow \operatorname{dlog}_\gamma x = a \equiv \psi(x)(\psi(\gamma))^{-1} \mod p-1. \end{aligned}$$

Si on dispose d'une méthode efficace pour calculer ψ, on obtient alors un algorithme efficace pour calculer le logarithme discret dans $\mathbb{Z}_p^*$ car les calculs dans $(\mathbb{Z}_{p-1}, +)$ sont simples à effectuer.

Remarque

- On ne connaît pas de méthode générale pour déterminer ψ pour un nombre premier arbitraire p.
- La détermination de ψ est aussi difficile que la détermination du logarithme discret.
- Si pour un groupe G quelconque, l'isomorphisme est facile à obtenir, il vaut mieux ne pas utiliser un tel groupe pour construire un cryptosystème.
- Pour des groupes construits sur des courbes elliptiques ou sur le groupe multiplicatif $\mathbb{F}_{p^f}^*$, on ne dispose pas de méthode générale de recherche de ψ.

Protocole d'échange des clés de Diffie-Hellman

Bob et Alice choisissent

- un grand nombre premier p
- une racine primitive γ modulo p.

Alice choisit un exposant a (secret) et envoie à Bob

$$A = \gamma^a \mod p.$$

Bob choisit un exposant b et envoie à Alice

$$B = \gamma^b \mod p.$$

Alice (connaissant a) peut calculer $B^a = \gamma^{ab} \mod p$
Bob (connaissant b) peut calculer $A^b = \gamma^{ab} \mod p$

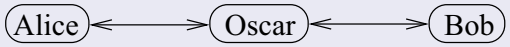
Cette valeur commune leur sert à présent de clé secrète commune.

Si Oscar espionne les échanges entre Alice et Bob, alors il a sa disposition les éléments suivants :

$$p,\ \gamma, A \text{ et } B.$$

Si le problème du logarithme discret est difficile, ne connaissant ni a ni b, il n'est pas en mesure de retrouver la clé secrète $B^a = A^b \mod p$.

Attaque "Man in the middle"



Pour se prémunir d'une telle attaque, il est dès lors nécessaire de recourir à un procédé de signature.

Cryptosystème d'ElGamal

Nous l'envisageons dans $\mathbb{Z}_p^*$ mais s'adapte à d'autres groupes ($\mathbb{F}_{p^f}^*$ ou groupes sur les courbes elliptiques).

Pour assurer la sécurité du cryptosystème, prendre $p \geq 2^{768}$.

On choisit un grand nombre premier p et $\gamma \in \mathbb{Z}_p^*$.

préférable mais pas nécessaire que γ soit une racine primitive modulo p.

Tirer γ au hasard

Dans $\mathbb{F}_p^*$, le nombre de générateurs est égal à $\varphi(p-1)$
J. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. of Math. **6***, 69–94, (1962).*

$$\forall n \geq 5,\ \varphi(n) \geq \frac{n}{\log\log n}.$$

En tirant un élément γ au hasard dans $\mathbb{Z}_p^*$, on a de "bonnes chances" qu'il s'agisse d'une racine primitive puisque la proportion de tels éléments dans $\mathbb{Z}_p^*$ est d'au moins $1/\log\log(p-1)$.

Tirer γ au hasard

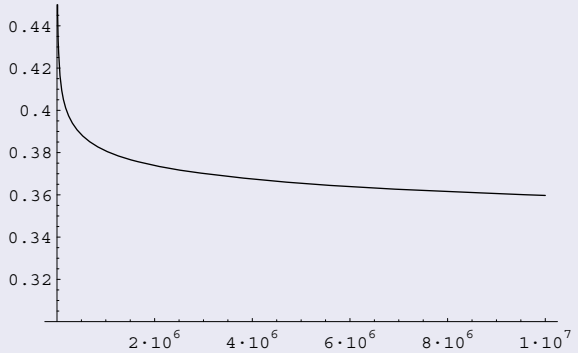


Fig.: Graphique de $1/\log\log x$ pour $x \leq 10^7$.

$1/\log\log 2^{768} \sim 0,1593$. Cette borne est la plus défavorable. Si $p-1 = 2.q$ avec q un nombre premier, alors $\varphi(p-1) = q-1$ et la probabilité de tirer au hasard une racine primitive est dès lors proche de $1/2$.

L'ensemble des textes clairs est $\mathcal{P} = \mathbb{Z}_p$ (on emploie, si nécessaire, des conventions de codage).

Bob choisit aléatoirement un exposant $0 < d < p-1$ (secret) et calcule

$$e = \gamma^d \mod p.$$

Bob publie

$$k = (p, \gamma, e).$$

On appelle parfois e la clé de Diffie-Hellman de Bob.

Si Alice veut envoyer un message x à Bob, elle choisit un nombre aléatoire $0 < b < p-1$ et envoie à Bob le couple

$$(\gamma^b \mod p,\ e^b x \mod p).$$

Remarque $e^b = (\gamma^d)^b = (\gamma^b)^d$.

Pour le déchiffrement, Bob reçoit $(\gamma^b \mod p,\ e^b x \mod p)$ et doit retrouver x.

Pour éviter de calculer $(e^b)^{-1} \mod p$ (ce qui, par ailleurs, est supposé difficile puisqu'il faudrait calculer le logarithme discret $\mathrm{dlog}_\gamma \gamma^b$ pour retrouver b),

Bob connaissant d, connaît aussi $p-1-d$ et il lui suffit alors de calculer $(\gamma^b)^{p-1-d} e^b x \mod p$ pour retrouver x. En effet,

$$(\gamma^b)^{p-1-d} e^b x \equiv (\gamma^{p-1})^b (\gamma^b)^{-d} e^b x$$

$$\equiv (\gamma^{p-1})^b (\gamma^b)^{-d} (\gamma^b)^d x \equiv x \mod p.$$

Que γ soit ou non une racine primitive modulo p, on a toujours $\gamma^{p-1} \equiv 1 \mod p$ car l'ordre d'un élément de $\mathbb{Z}_p^*$ divisant l'ordre du groupe, $p-1$ est un multiple de l'ordre de γ.

Calculs nécessaires

Du même type que pour le RSA, mais le RSA est bien plus lent.

Il s'agit simplement d'exponentiations modulaires. Le déchiffrement nécéssite une exponentiation et le chiffrement en nécéssite deux.

Cependant, les calculs de $\gamma^b \mod p$ et $e^b \mod p$ peuvent être réalisés une fois pour toutes par Alice (elle choisit un seul b pour tous ces textes clairs x) et donc être supposés précalculés.

Par conséquent, le chiffrement d'ElGamal ne nécéssite en fin de compte qu'une multiplication modulo p ce qui est de loin bien plus efficace que le RSA.

```
p = Prime[123456789]

2543568463

gamma = Prime[12345678]

224284387

d = 12345678

12345678

e = PowerMod[gamma, d, p]

831108609

texteclair =
 "une douleur foudroyante lui traversa la tete,une douleur comme il n'en avait
   encore jamais ressenti. c'etait comme si sa cicatrice avait soudain pris feu."

une douleur foudroyante lui traversa la tete,une douleur comme il n'en avait
  encore jamais ressenti. c'etait comme si sa cicatrice avait soudain pris feu.

N[Log[32, p]]

6.24884
```

codetxclair = code[texteclair]

```
{21, 14, 5, 0, 4, 15, 21, 12, 5, 21, 18, 0, 6, 15, 21, 4, 18, 15, 25, 1, 14, 20, 5, 0, 12, 21,
 9, 0, 20, 18, 1, 22, 5, 18, 19, 1, 0, 12, 1, 0, 20, 5, 20, 5, 27, 21, 14, 5, 0, 4, 15,
 21, 12, 5, 21, 18, 0, 3, 15, 13, 13, 5, 0, 9, 12, 0, 14, 29, 5, 14, 0, 1, 22, 1, 9, 20,
 0, 5, 14, 3, 15, 18, 5, 0, 10, 1, 13, 1, 9, 19, 0, 18, 5, 19, 19, 5, 14, 20, 9, 28, 0, 3,
 29, 5, 20, 1, 9, 20, 0, 3, 15, 13, 13, 5, 0, 19, 9, 0, 19, 1, 0, 3, 9, 3, 1, 20, 18, 9,
 3, 5, 0, 1, 22, 1, 9, 20, 0, 19, 15, 21, 4, 1, 9, 14, 0, 16, 18, 9, 19, 0, 6, 5, 21, 28}
```

Length[codetxclair]

```
154
```

codetxclair = ajout[codetxclair, 6]

```
{21, 14, 5, 0, 4, 15, 21, 12, 5, 21, 18, 0, 6, 15, 21, 4, 18, 15, 25, 1, 14, 20, 5, 0, 12, 21, 9,
 0, 20, 18, 1, 22, 5, 18, 19, 1, 0, 12, 1, 0, 20, 5, 20, 5, 27, 21, 14, 5, 0, 4, 15, 21,
 12, 5, 21, 18, 0, 3, 15, 13, 13, 5, 0, 9, 12, 0, 14, 29, 5, 14, 0, 1, 22, 1, 9, 20, 0, 5,
 14, 3, 15, 18, 5, 0, 10, 1, 13, 1, 9, 19, 0, 18, 5, 19, 19, 5, 14, 20, 9, 28, 0, 3, 29,
 5, 20, 1, 9, 20, 0, 3, 15, 13, 13, 5, 0, 19, 9, 0, 19, 1, 0, 3, 9, 3, 1, 20, 18, 9, 3, 5,
 0, 1, 22, 1, 9, 20, 0, 19, 15, 21, 4, 1, 9, 14, 0, 16, 18, 9, 19, 0, 6, 5, 21, 28, 0, 0}
```

liste = codebloc[codetxclair, 6]

```
{719487119, 717411904, 217748047, 840388768, 424968850, 56805985,
 12616325, 677238213, 4707717, 723521005, 441460096, 500348929,
 739561477, 473417888, 337020211, 19058277, 491057155, 978978100, 3650981,
 20218465, 3443764, 613520385, 739561491, 525468974, 17376864, 207286272}
```

b = Random[Integer, {1, p - 1}]

```
2077626273
```

PowerMod[gamma, b, p]

```
2174065976
```

temp = PowerMod[e, b, p]

```
401303819
```

codetxchiffre = Mod[temp * liste, p]

```
{1224703372, 1813996580, 879587936, 965469907, 1572901588, 1078313219, 1291506749,
 397171217, 2052820288, 1630733064, 162334271, 1346975257, 1481548401,
 31283547, 452298537, 2531435220, 2538016017, 2419180759, 1225202253, 373714894,
 1135501389, 1561257229, 2012664941, 1607195455, 371515150, 1134385436}
```

decodebloc[codetxchiffre, 7]

```
ado:?llava:yad zfz.s  .xwyvsan.advta dkphcafouua' kzxvpqa'ewcj
  apsf xh dzzaq?ahdrmpyald'hsq  'zvj, mokayibknehvtbktnchqbhccqfwadpnfrm
  kdl,:naaz.xbmanp'yhma,?mucmao.wvy? kbiwxnaayzvh.
```

temp = PowerMod[2174065976, (p - 1 - d), p]

```
438045370
```

Mod[temp * codetxchiffre, p]

```
{719487119, 717411904, 217748047, 840388768, 424968850, 56805985,
 12616325, 677238213, 4707717, 723521005, 441460096, 500348929,
 739561477, 473417888, 337020211, 19058277, 491057155, 978978100, 3650981,
 20218465, 3443764, 613520385, 739561491, 525468974, 17376864, 207286272}
```