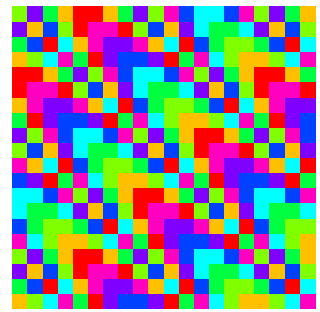
Mathématiques Discrètes

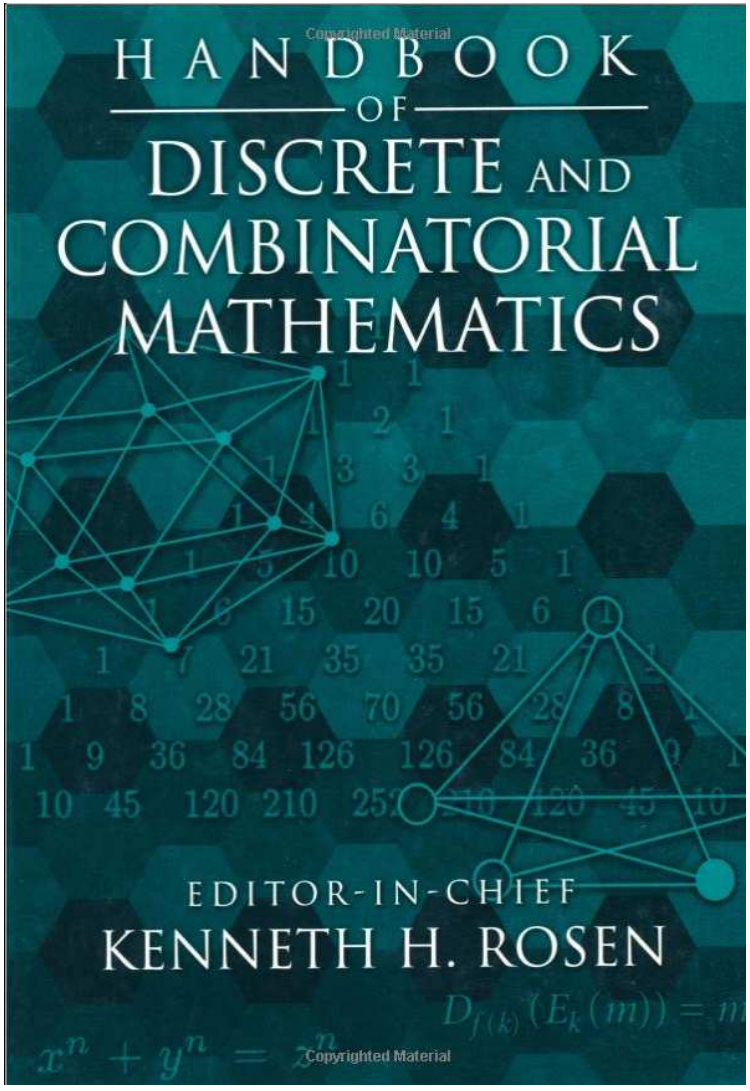
Michel Rigo
en co-titulariat avec Emilie Charlier

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

Année 2016–2017



Qu'est-ce que les *mathématiques discrètes* ?



Some topics. . .

Counting Methods.
Sequences.
Number Theory.
Algebraic Structures.
Discrete Probability.
Graph Theory
Partially Ordered Sets.
Combinatorial Designs.
Discrete Geometry.
Coding Theory.
Cryptology.
Discrete Optimization.
Theoretical Computer Science.
Information Structures.
Data Mining.

Avec des conventions de *codage* partagées/connues, on peut "tout coder" par des suites d'éléments appartenant à une structure algébrique finie ($\mathbb{Z}_n$, corps fini, monoïde finiment engendré, ...) :

- textes (.doc, .rtf, SMS, html, RSS, ...)
- images, photos (.jpg, .png, .bmp, MMS, ...)
- sons, musique (CD, .wav, .mp3, ...)
- vidéos (DVD, .mov, .mpg, .divx, .mp4, ...)

Exemple : codage ASCII

bijection entre un alphabet $\mathcal{A}$ et $\mathbb{Z}_{256}$

bijection entre $\mathcal{A}^{\mathbb{N}}$ et $(\mathbb{Z}_{256})^{\mathbb{N}}$

Code ASCII *American Standard Code for Information Interchange*

1 ┌	33 !	65 A	97 a	129 ▯	161 ¡	193 Á	225 á
2 ┐	34 "	66 B	98 b	130 ‚	162 ¢	194 Â	226 â
3 └	35 #	67 C	99 c	131 ƒ	163 £	195 Ã	227 ã
4 ┘	36 $	68 D	100 d	132 „	164 ¤	196 Ä	228 ä
5 |	37 %	69 E	101 e	133 …	165 ¥	197 Å	229 å
6 ─	38 &	70 F	102 f	134 †	166 ¦	198 Æ	230 æ
7 •	39 '	71 G	103 g	135 ‡	167 §	199 Ç	231 ç
8 ◘	40 (	72 H	104 h	136 ˆ	168 ¨	200 È	232 è
9	41)	73 I	105 i	137 ‰	169 ©	201 É	233 é
10	42 *	74 J	106 j	138 Š	170 ª	202 Ê	234 ê
11 ♂	43 +	75 K	107 k	139 ‹	171 «	203 Ë	235 ë
12 ▫	44 ,	76 L	108 l	140 Œ	172 ¬	204 Ì	236 ì
13	45 -	77 M	109 m	141 ▯	173 -	205 Í	237 í
14 ♫	46 .	78 N	110 n	142 Ž	174 ®	206 Î	238 î
15 ☼	47 /	79 O	111 o	143 ▯	175 ¯	207 Ï	239 ï
16 ►	48 0	80 P	112 p	144 ▯	176 °	208 Ð	240 ð
17 ◄	49 1	81 Q	113 q	145 '	177 ±	209 Ñ	241 ñ
18 ↕	50 2	82 R	114 r	146 '	178 ²	210 Ò	242 ò
19 ‼	51 3	83 S	115 s	147 "	179 ³	211 Ó	243 ó
20 ¶	52 4	84 T	116 t	148 "	180 ´	212 Ô	244 ô
21 §	53 5	85 U	117 u	149 •	181 µ	213 Õ	245 õ
22 ▬	54 6	86 V	118 v	150 –	182 ¶	214 Ö	246 ö
23 ↨	55 7	87 W	119 w	151 —	183 ·	215 ×	247 ÷
24 ↑	56 8	88 X	120 x	152 ˜	184 ¸	216 Ø	248 ø
25 ↓	57 9	89 Y	121 y	153 ™	185 ¹	217 Ù	249 ù
26 →	58 :	90 Z	122 z	154 š	186 º	218 Ú	250 ú
27 ←	59 ;	91 [	123 {	155 ›	187 »	219 Û	251 û
28	60 <	92 \	124 |	156 œ	188 ¼	220 Ü	252 ü
29	61 =	93]	125 }	157 ▯	189 ½	221 Ý	253 ý
30	62 >	94 ^	126 ~	158 ž	190 ¾	222 Þ	254 þ
31	63 ?	95 _	127 ⌂	159 Ÿ	191 ¿	223 ß	255 ÿ
32	64 @	96 `	128 €	160	192 À	224 à	

Code ASCII

Savoir compter
de 0 à 255
en base 2...

65 A	97 a
66 B	98 b
67 C	99 c
68 D	100 d
69 E	101 e
70 F	102 f
71 G	103 g
72 H	104 h
73 I	105 i
74 J	106 j
75 K	107 k
76 L	108 l
77 M	109 m
78 N	110 n
79 O	111 o
80 P	112 p
81 Q	113 q
82 R	114 r
83 S	115 s
84 T	116 t
85 U	117 u

128	-64	-32	-16	- 8	- 4	- 2	- 1	
0	0	0	0	0	0	0	0 =	0
0	0	0	0	0	0	0	1 =	1
								...
0	1	0	0	0	0	1	0 =	66
								...
0	1	1	0	1	0	1	0 =	106
								...
1	1	1	1	1	1	1	1 =	255

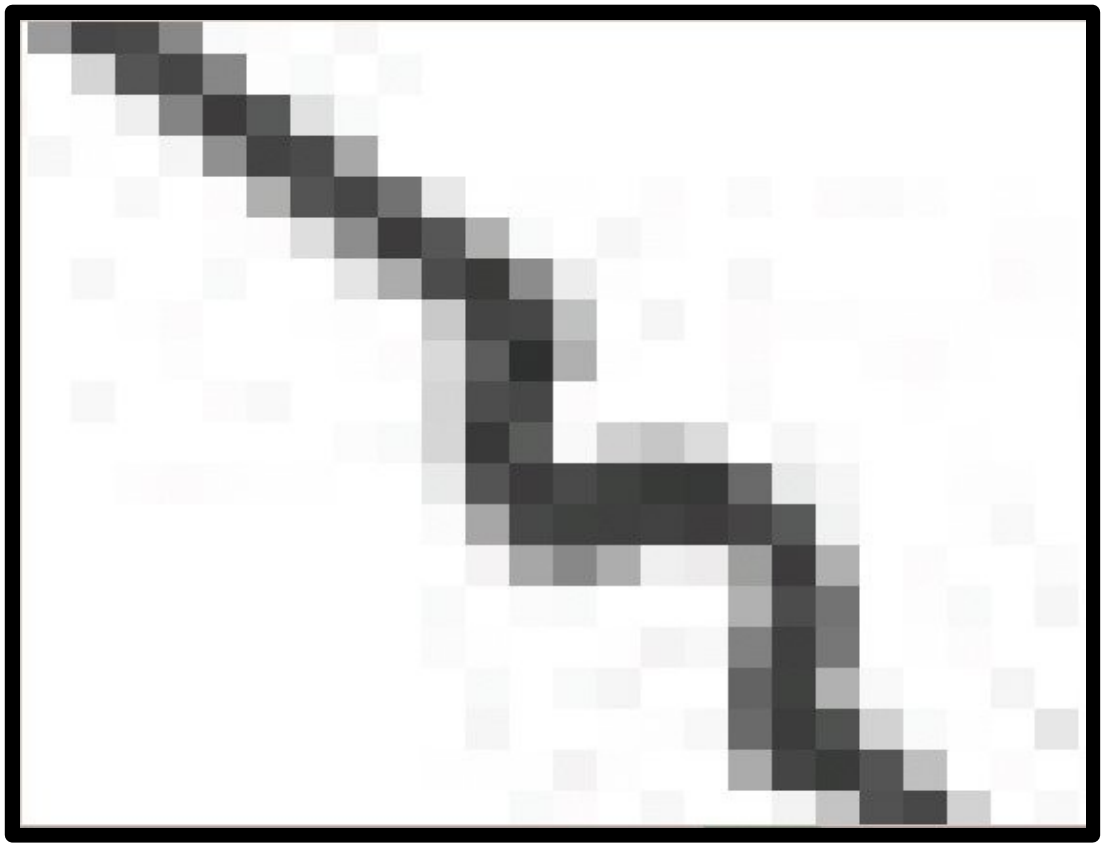
Bonjour

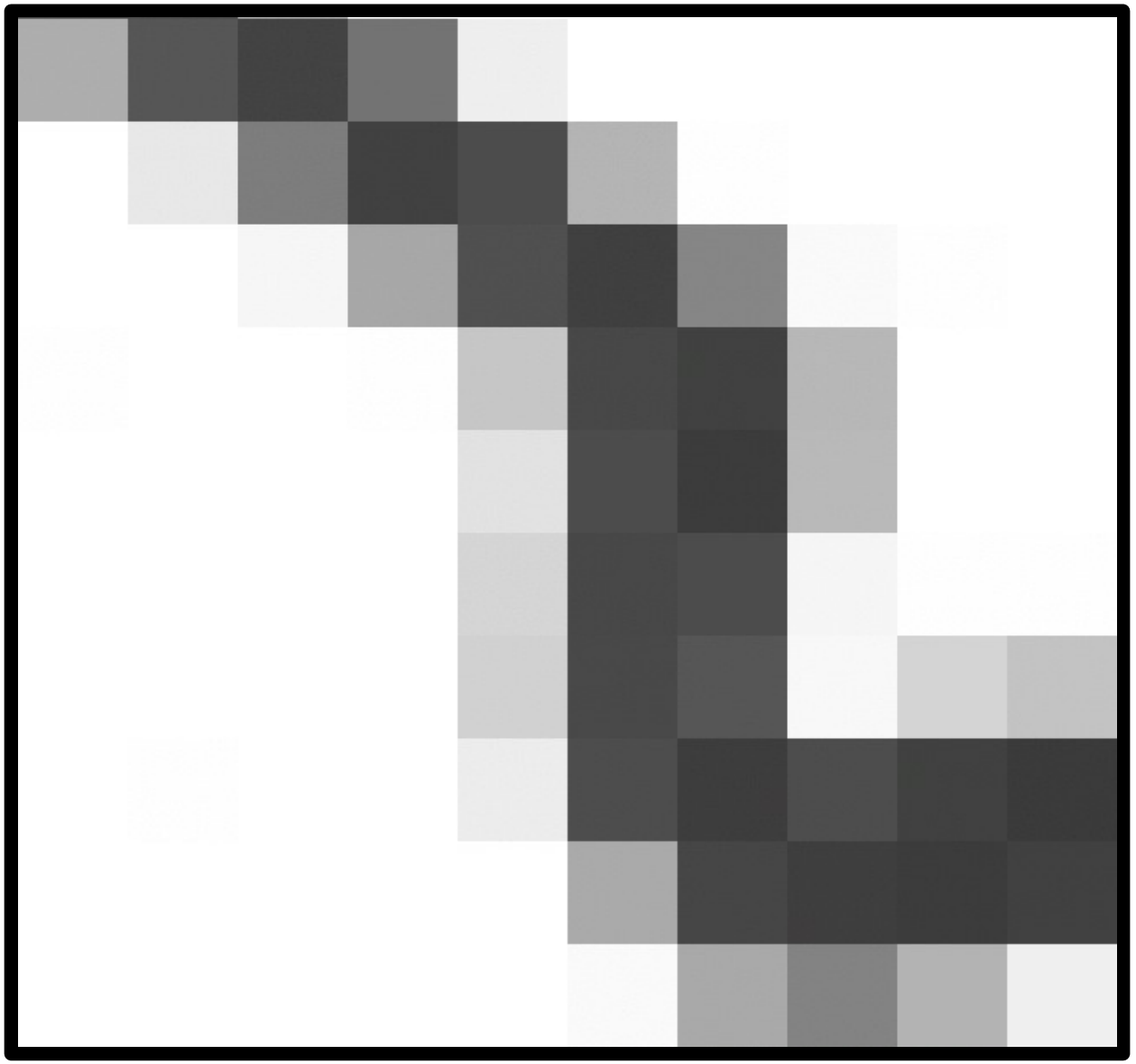
66, 111, 110, 106, 111, 117, 114

01000010 01101111 01101110 01101010
01101111 01110101 01110010

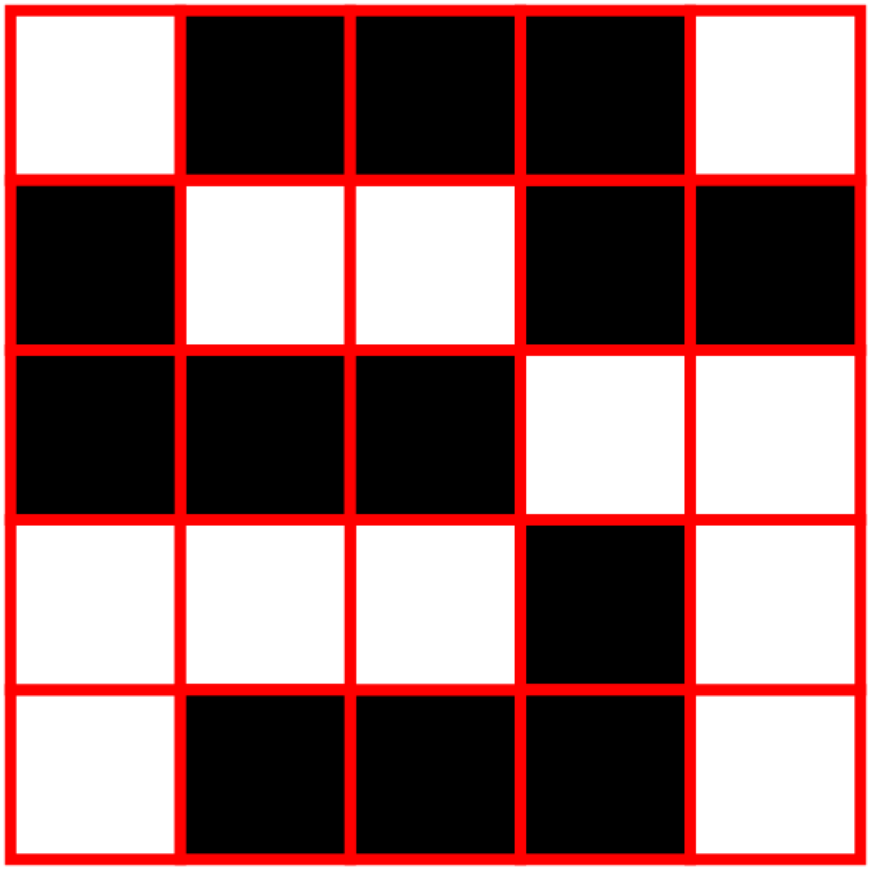
Coder des images avec des 0 et des 1...


MOI
À
L'ÉCOLE
EN
ALGÈBRE

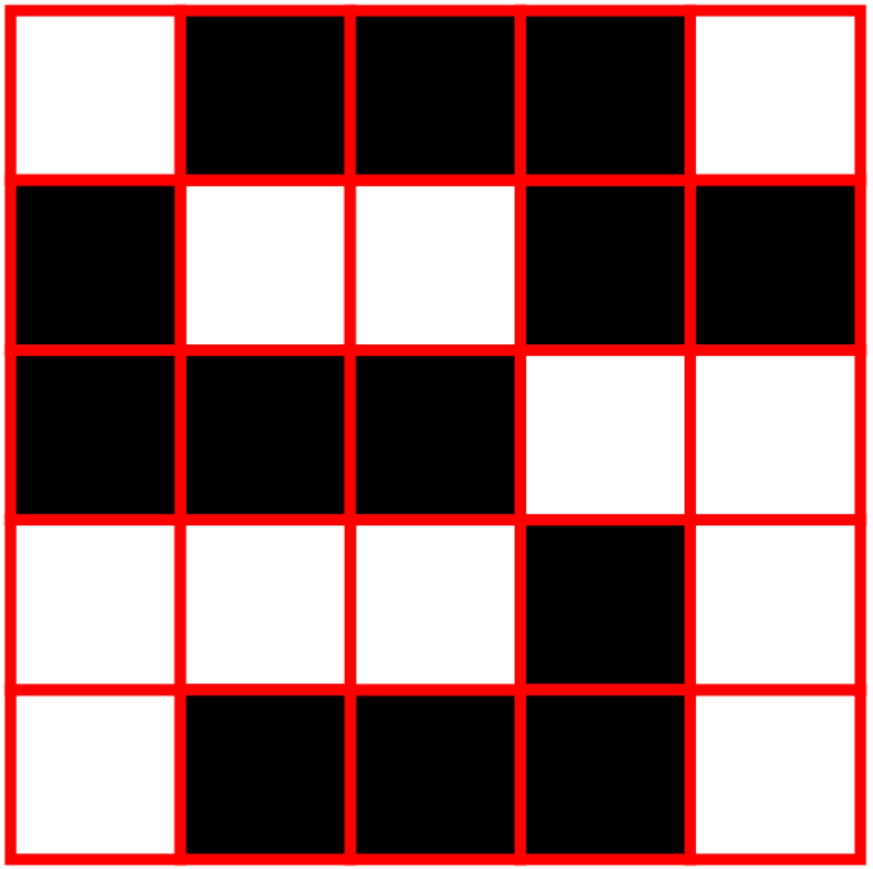




Images en noir et blanc

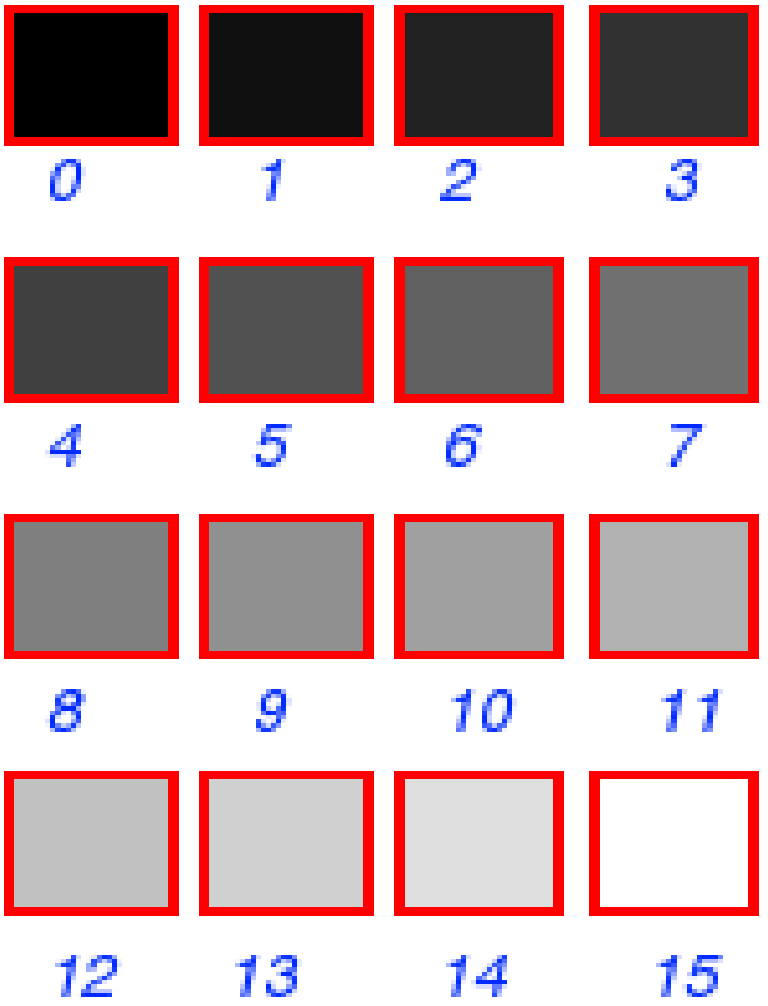


Images en noir et blanc

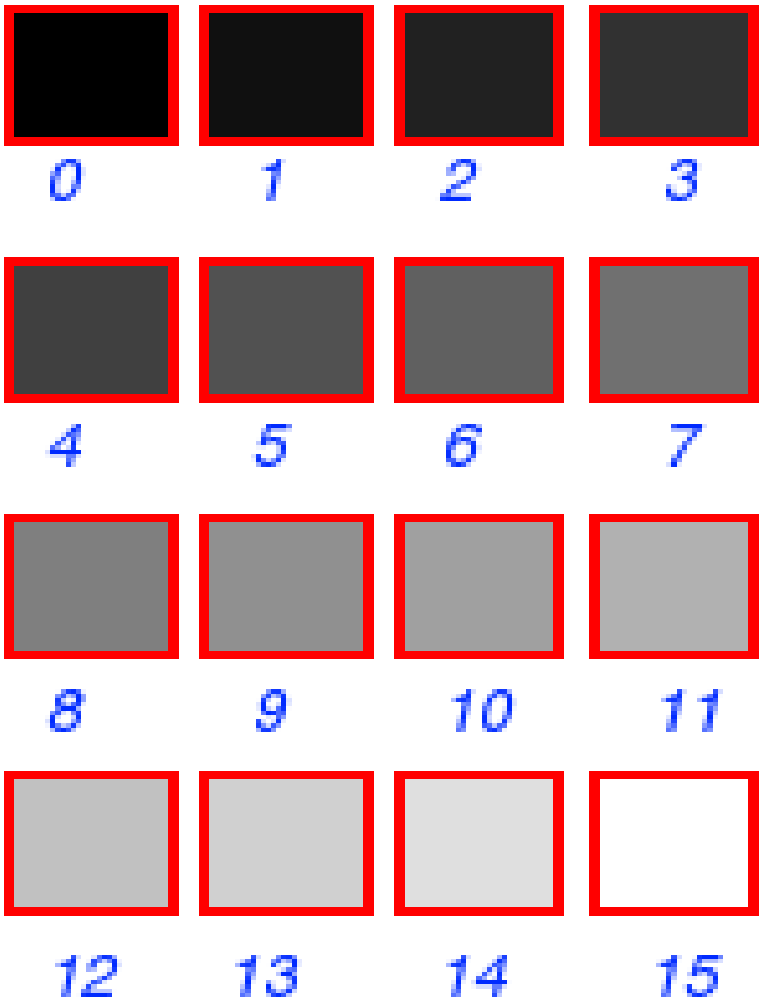


1 0 0 0 1
0 1 1 0 0
0 0 0 1 1
1 1 1 0 1
1 0 0 0 1

Images en 16 dégradés de gris



Images en 16 dégradés de gris

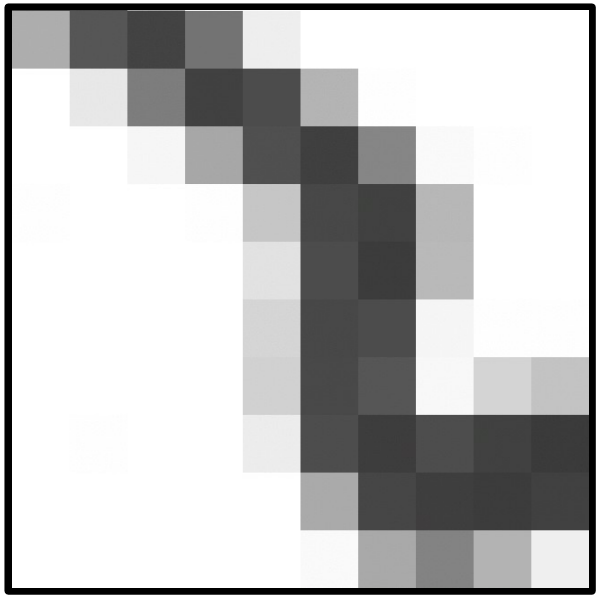


0000 0001 0010 0011

0100 0101 0110 0111

1000 1001 1010 1011

1100 1101 1110 1111



1011 0110 0100 1001 1110 1111 1111 1111 1111 1111
1111 1110 0111 0100 0101 1010 1111 1111 1111 1111
1111 1111 1110 1000 0101 0100 1001 1111 1111 1111
1111 1111 1111 1111 1010 0101 0100 1011 1111 1111
1111 1111 1111 1111 1011 0101 0011 1011 1111 1111

...

Et pour les images
en couleur ...

01101100 11001110
11000000 10101010
00010100 11001100 ...

00111100 01000111
01010101 00101111
11001110 10101100 ...

01111100 10001010
11010110 10101110
01110101 01011100 ...

Organisation de cette partie

- Rappels et compléments sur les corps finis
- Constructions et prise en main dans `Mathematica`
- Arithmétique et complexité des opérations sur un corps fini
- Cryptographie à clé secrète
- Cryptographie à clé publique

Quotient d'un anneau par un idéal

Soient $(A, +, \cdot, 0, 1)$ 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 est la classe $0 + I = I$

$$a + I = b + I \Leftrightarrow a - b \in I.$$

Rappels sur les corps finis

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.

Théorème de Wedderburn

Tout corps fini est commutatif : *corps fini et champ fini sont des synomynes*.

Rappels sur les corps finis

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.

Théorème

Soient $\mathbb{K}$ un champ. L'anneau $\mathbb{K}[X]$ 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.

Proposition (construction de corps)

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

Rappels sur les corps finis

$\mathbb{Z}_3[X]$ 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 sur les corps finis

Table de multiplication (sans 0) — version 1

$\cdot$	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	$2X$

Table de multiplication (sans 0)

version 2 (liste des coefficients)

$\cdot$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,1)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$	$(2,0)$	$(2,1)$	$(2,2)$
$(0,2)$	$(0,2)$	$(0,1)$	$(2,0)$	$(2,2)$	$(2,1)$	$(1,0)$	$(1,2)$	$(1,1)$
$(1,0)$	$(1,0)$	$(2,0)$	$(0,2)$	$(1,2)$	$(2,2)$	$(0,1)$	$(1,1)$	$(2,1)$
$(1,1)$	$(1,1)$	$(2,2)$	$(1,2)$	$(2,0)$	$(0,1)$	$(2,1)$	$(0,2)$	$(1,0)$
$(1,2)$	$(1,2)$	$(2,1)$	$(2,2)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(0,1)$
$(2,0)$	$(2,0)$	$(1,0)$	$(0,1)$	$(2,1)$	$(1,1)$	$(0,2)$	$(2,2)$	$(1,2)$
$(2,1)$	$(2,1)$	$(1,2)$	$(1,1)$	$(0,2)$	$(2,0)$	$(2,2)$	$(1,0)$	$(0,1)$
$(2,2)$	$(2,2)$	$(1,1)$	$(2,1)$	$(1,0)$	$(0,2)$	$(1,2)$	$(0,1)$	$(2,0)$

Rappels sur les corps finis

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

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

$\cdot$	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 sur les corps finis

Si $p \geq 2$ premier et $P \in \mathbb{Z}_p[X]$ polynôme irréductible de degré f, alors

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

est un champ à p^f éléments.

Questions :

- nombre d'éléments d'un champ fini arbitraire ?
- Peut-on obtenir tous les champs finis de cette façon ?
- existence de polynômes irréductibles pour tout $f \geq 1$?

Remarque

Construction alternative d'un champ fini en considérant l'extension d'un champ $\mathbb{K}$ par un élément algébrique α, $\mathbb{K}[X]/\langle M_\alpha \rangle \cong \mathbb{K}(\alpha)$.

Rappels sur les corps finis

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

homomorphisme caractéristique :

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

et $\Phi(m) = -\Phi(-m)$, si $m < 0$.

Φ est entièrement caractérisé par $\Phi(1_{\mathbb{Z}}) = 1_{\mathbb{K}}$.

$\ker \Phi$ est un idéal de $\mathbb{Z}$ et l'anneau $\mathbb{Z}$ est principal.

Définition

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

Rappels sur les corps finis

Premier théorème d'isomorphie : $\mathbb{Z}/\ker\Phi$ isomorphe à $\operatorname{Im}\Phi \subset \mathbb{K}$

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

$\mathbb{Z}/\ker\Phi = \mathbb{Z}$ s'identifie à un sous-anneau de $\mathbb{K}$.
donc $\mathbb{K}$ est infini et contient un sous-champ $\widetilde{=} \mathbb{Q}$.

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

Or Φ est un homomorphisme et on doit avoir $\Phi(1) = 1$.
On aurait $0 = 1$. Impossible dans un champ.

Rappels sur les corps finis

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

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

Rappel

$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ intègre (et même un champ) SSI $n > 1$ est premier.

La caractéristique n de $\mathbb{K}$ (fini ou infini) est un nombre premier.

$\mathbb{K}$ contient un sous-champ $\cong \mathbb{Z}_n$, i.e., $\mathbb{K}$ est une extension de $\mathbb{Z}_n$.

Conclusion

La caractéristique d'un champ fini est un nombre premier $p \geq 2$.

Rappels sur les corps finis

Proposition

Soit $\mathbb{K}$ un champ fini de caractéristique $p \geq 2$.
Il existe $f \geq 1$ tel que $\mathbb{K}$ contienne exactement p^f éléments.

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

$\mathbb{K}$ vu comme un $\mathbb{Z}_p$-vectoriel. Si $[\mathbb{K} : \mathbb{Z}_p] = f$, alors $\#\mathbb{K} = p^f$.

En effet, si $(k_1, \ldots, k_f)$ est une base de $\mathbb{K}$, alors tout élément de $\mathbb{K}$ est de la forme

$$z_1\, k_1 + \cdots + z_f\, k_f$$

avec les $z_i \in \mathbb{Z}_p$. ■

Rappels sur les corps finis

Corollaire

Un champ fini $\mathbb{K}$ contient un unique *champ* de la forme $\mathbb{Z}_q$ ($q \geq 2$ premier).

Si $\operatorname{car} \mathbb{K} = p$, i.e., $\mathbb{K}$ contient un sous-champ isomorphe à $\mathbb{Z}_p$, $\mathbb{K}$ contient p^f éléments (vu le résultat préc.)

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

Conclusion

Pour tout champ fini $\mathbb{K}$, il existe un unique p premier tel que $\mathbb{K}$ contient une copie de $\mathbb{Z}_p$ appelée le sous-champ premier de $\mathbb{K}$.

En particulier, p coïncide avec la caractéristique de $\mathbb{K}$.

Rappels sur les corps finis

Existence et unicité (à isomorphisme près) d'un corps à p^f éléments.

Théorème

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.

Théorème

Soit $\mathbb{F}$ un champ à $q = p^f$ éléments.

Tout élément de $\mathbb{F}$ satisfait l'équation $X^q - X = 0$;
$\mathbb{F}$ est précisément l'ensemble des racines de cette équation.

C.à.d, pour tout sous-champ $\mathbb{K}$ de $\mathbb{F}$ (en particulier, $\mathbb{K} = \mathbb{Z}_p$),
$\mathbb{F}$ est le corps de rupture du polynôme $X^q - X$ sur $\mathbb{K}$.

Notation : $\mathbb{F}_q$ ou $GF(q)$

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 $d|f$.

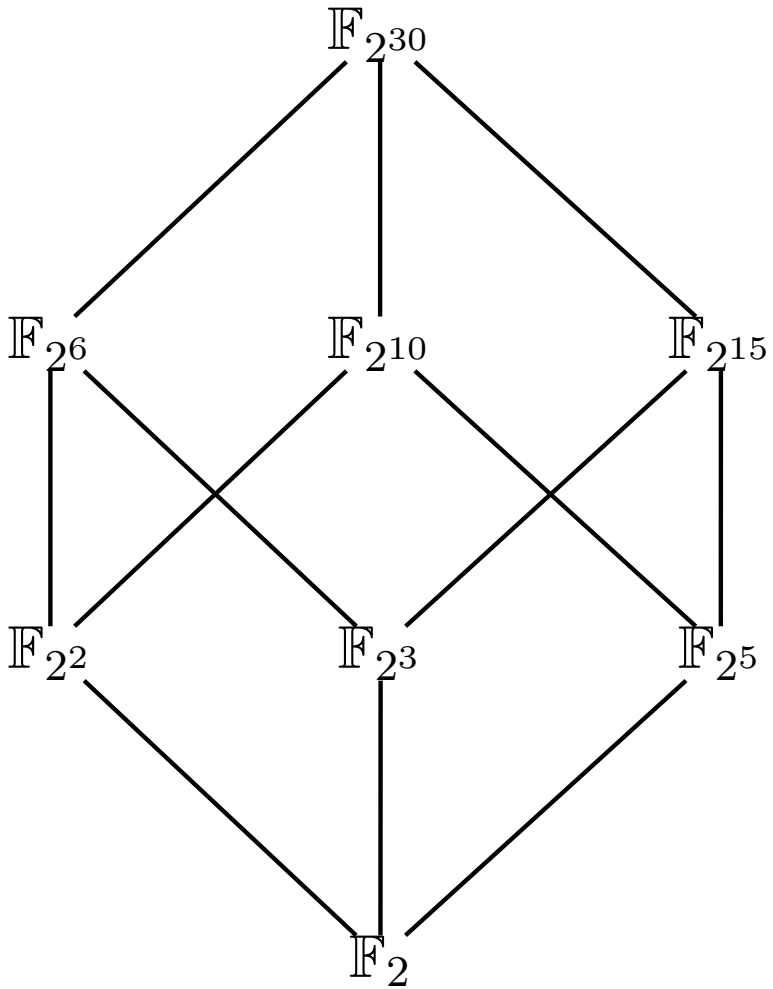
Plus précisément, si $\mathbb{K}$ est un sous-champ de $\mathbb{F}_q$, alors il contient p^d éléments où d divise f.

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 $\mathbb{F}_{p^d}$.

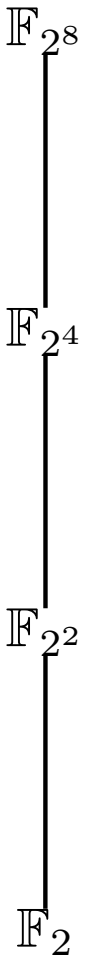
Strucuture des corps finis

diviseurs de 30 : $1, 2, 3, 5, 6, 10, 15, 30$



Structure des corps finis

$\mathbb{F}_{2^8} = \mathbb{F}_{256}$, diviseurs de 8 : $1, 2, 4, 8$,



Structure (multiplicative) des corps finis

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

$$\mathbb{F}_q^* = \{g^n \mid n = 1, \ldots, q-1\}.$$

Exemple

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

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

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 (multiplicative) des corps finis

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

Théorème

- Tout champ fini $\mathbb{F}_q$ possède un générateur.
- Soit 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 $\varphi(q-1)$.

La preuve de ce résultat apporte un élément intéressant :

Pour tout diviseur d de $q-1$,
$\mathbb{F}_q^*$ contient $\varphi(d)$ éléments d'ordre d.

Structure (multiplicative) des corps finis

Lemme

$$\forall N \geq 2, \quad \sum_{d|N} \varphi(d) = N.$$

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.

On en tire donc

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

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

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

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.
Ainsi, lorsqu'on parcourt l'ensemble des N/d_i possibles,
on parcourt en fait l'ensemble de tous les diviseurs de N. ■

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 (multiplicative) des corps 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 (multiplicative) des corps finis

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

$a, a^2, \ldots, a^d$ 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 $\mathrm{pgcd}(j,d)=d'>1$, 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 $\mathrm{pgcd}(j,d)=1$, $\exists\ u,\ v : 1=ju-dv,\ a=a^{1+dv}=(a^j)^u$

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

Structure (multiplicative) des corps 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, $k \leq \ell$.

Conclusion des parties 1 et 2 : 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 (multiplicative) des corps 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 $q - 1$. ■

Structure (multiplicative) des corps finis

Illustration

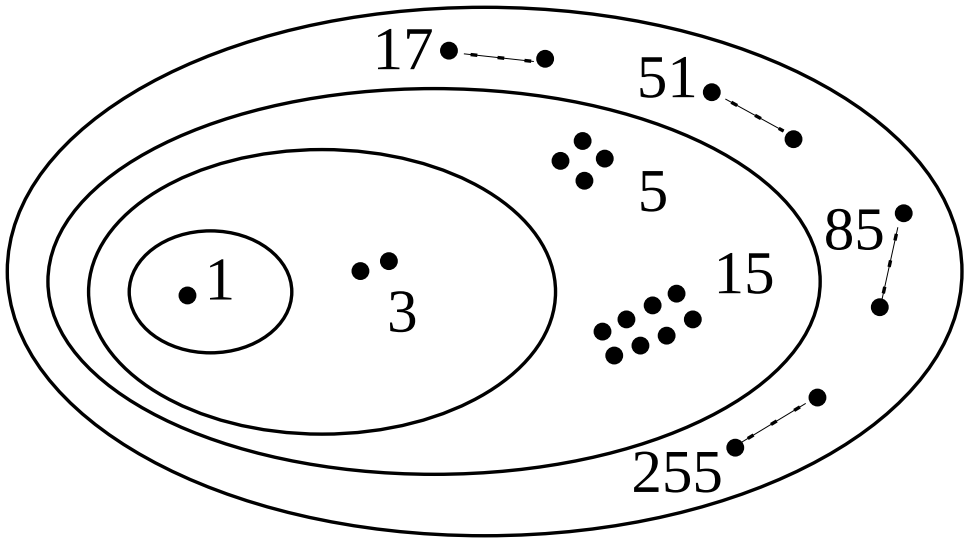
$\mathbb{F}_9 = \mathbb{Z}_3[X]/\langle X^2+1\rangle$

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).

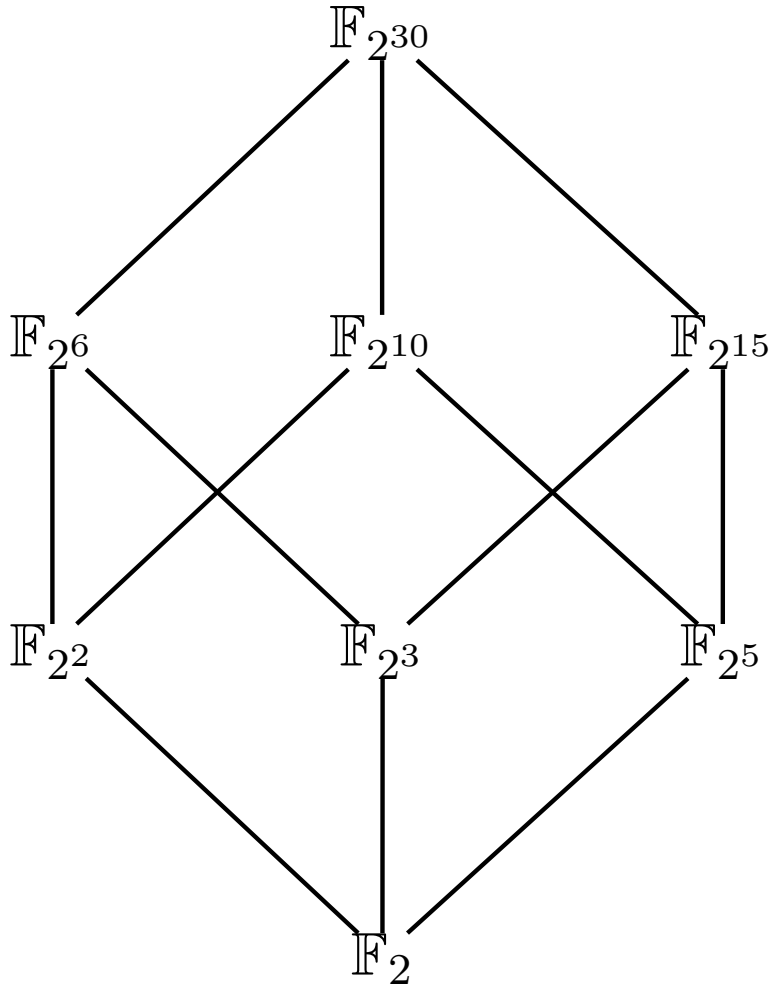
Deux exemples, reprenons $\mathbb{F}_{2^8} \supset \mathbb{F}_{2^4} \supset \mathbb{F}_{2^2} \supset \mathbb{F}_2$.
Peut-on déterminer le nombre d'éléments de chaque ordre ?

	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



Dans ce tableau, tous les éléments repris dans les k premières lignes appartiennent aussi aux sous-champs apparaissant "plus bas" (à cause de l'emboîtement).

Deuxième exemple $\mathbb{F}_{2^{30}}$

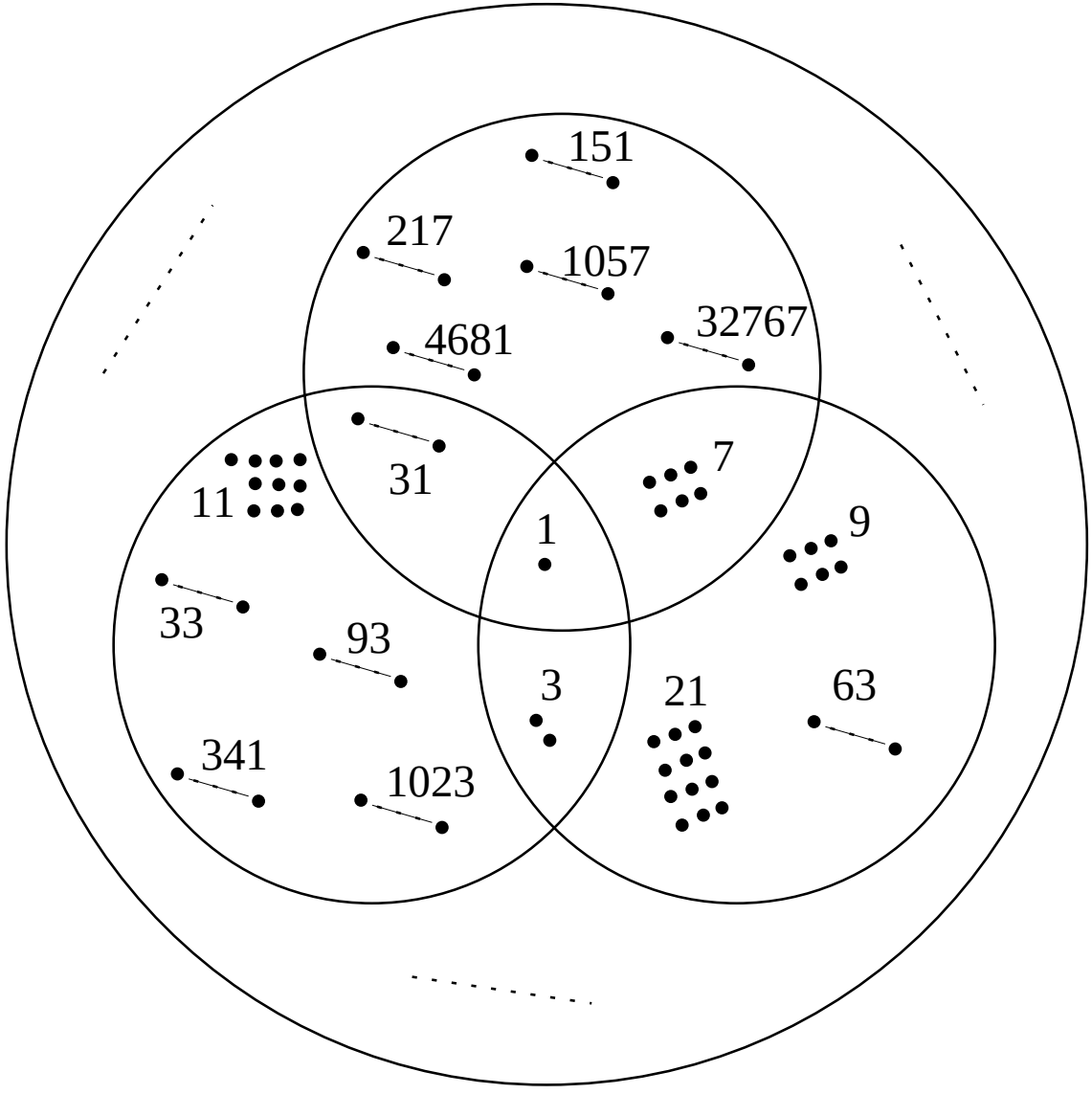


$\mathbb{F}_{2^6} \supset \mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^3}$; $\mathbb{F}_{2^{10}} \supset \mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^3}$

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

$\mathbb{F}_{2^{15}} \supset \mathbb{F}_2, \mathbb{F}_{2^3}, \mathbb{F}_{2^5}$

	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	
	$\vdots$	$\vdots$	
	1073741823	534600000	


151
217
1057
32767
4681
31
11
7
1
9
33
93
3
21
63
341
1023

Polynômes irréductibles

Théorème $q = p^f$

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

Dans $\mathbb{Z}_3[X]$, on a

$$(X^2+1).(X^2+X+2).(X^2+2X+2).X.(X+1).(X+2) = X^9 - X$$

Polynômes irréductibles

Corollaire

Si 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 sur $\mathbb{F}_p$.

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 : $X - \alpha$, pour $\alpha \in \mathbb{F}_p$

Polynômes irréductibles

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

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

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

i.e.,

$$N_p(f) = \frac{p^f - p}{f}$$

■

Polynômes irréductibles

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

Au vu du thm.

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

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

Polynômes irréductibles

Calculer de proche en proche $N_p(f)$ est . . . "rassurant"

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

Proportion du nombre de polynômes irréductibles

Remarque (1)

On peut montrer que

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

Remarque (2)

Pour tout $f > 2$, on peut assez facilement [1] montrer que

$$N_p(f) \geq \frac{p^f - p\sqrt{p^f}}{f}.$$

1. $\mathbb{K} \subset \mathbb{L}$ deux champs ; $\alpha \in \mathbb{L}$ est un *générateur* de $\mathbb{L}$ sur $\mathbb{K}$ si $\mathbb{L} = \mathbb{K}[\alpha]$.

Polynômes irréductibles

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.

- M. Butler, Quart. J. Math. Oxford, 1954
- M. O. Rabin, Probabilistic algorithms in finite fields, 1980
- M. Ben-Or, Probabilistic algorithms in finite fields, 1981
- V. Shoup, Fast construction of irreducible polynomials over finite fields, 1995

`The problem of finding irreducible polynomials over finite fields is an important problem in algorithmic algebra with many applications in coding theory, cryptography and complexity theory. In many such applications the primary use of irreducible polynomials is in the construction of larger finite fields.` [C. Saha]