MATHÉMATIQUES DISCRÈTES (3)

Michel Rigo

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

Année 2007–2008

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 $\mathbb{Z}_n$.)

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 $\mathbb{K}$.

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)

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

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

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

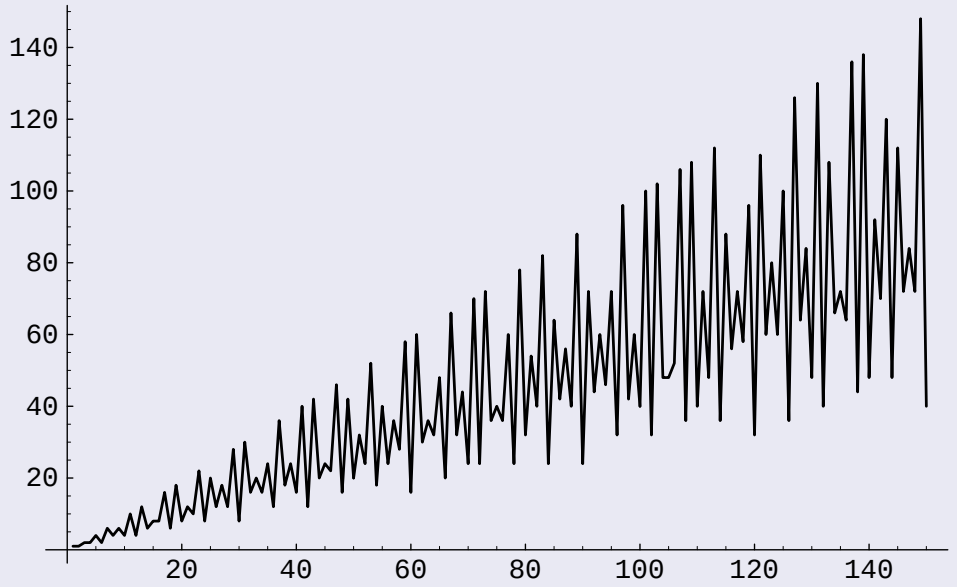
L. Euler

DÉFINITION

Fonction indicatrice d'Euleur ou fonction totient

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

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



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 $\simeq$ 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

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 $p^k - p^{k-1} = (p-1)\,p^{k-1}$.

PETIT THÉORÈME DE FERMAT / EULER

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

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

$\text{pgcd}(a, m) = 1$ 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 $\text{pgcd}(a, m) = 1$, alors $\text{pgcd}(a', m) = 1$ et $a \equiv a' \mod m$.

Autre formulation, cas particulier

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

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

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 $(m-1)! \mod m \ldots$

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 $\text{pgcd}(j, q-1) = 1$.
- Le nombre de générateurs de $\mathbb{F}_q$ est $\varphi(q-1)$.

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.

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

$1 \leq k \leq N$ 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

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

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.

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

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

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

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.

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.

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**

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

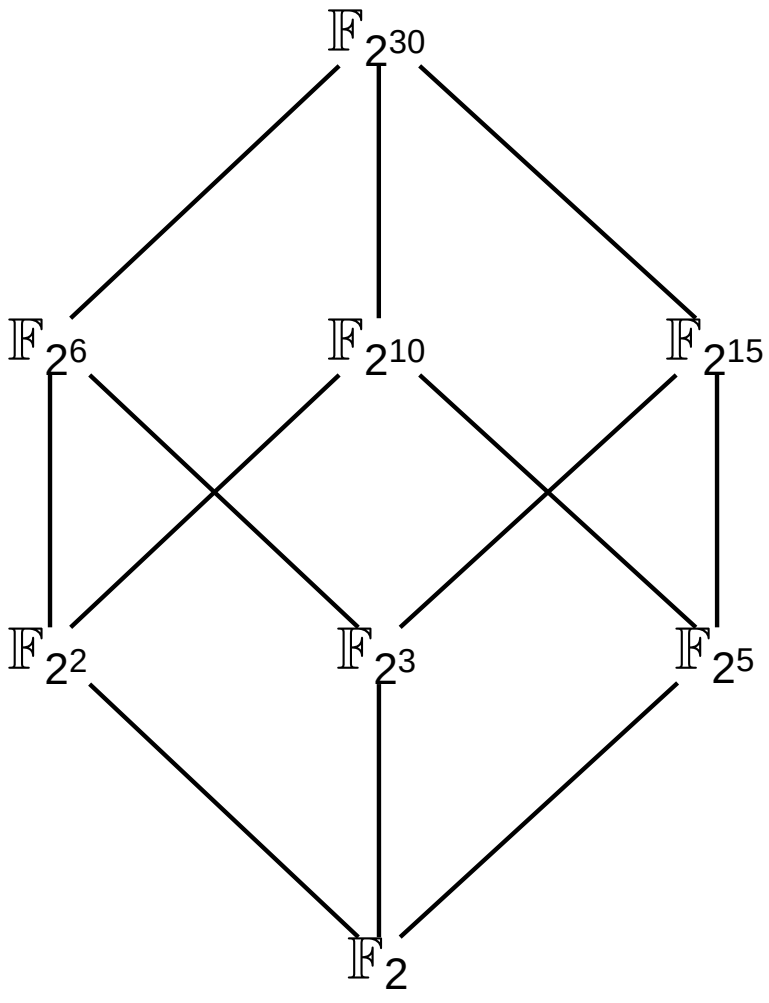
$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha).$$

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 ?

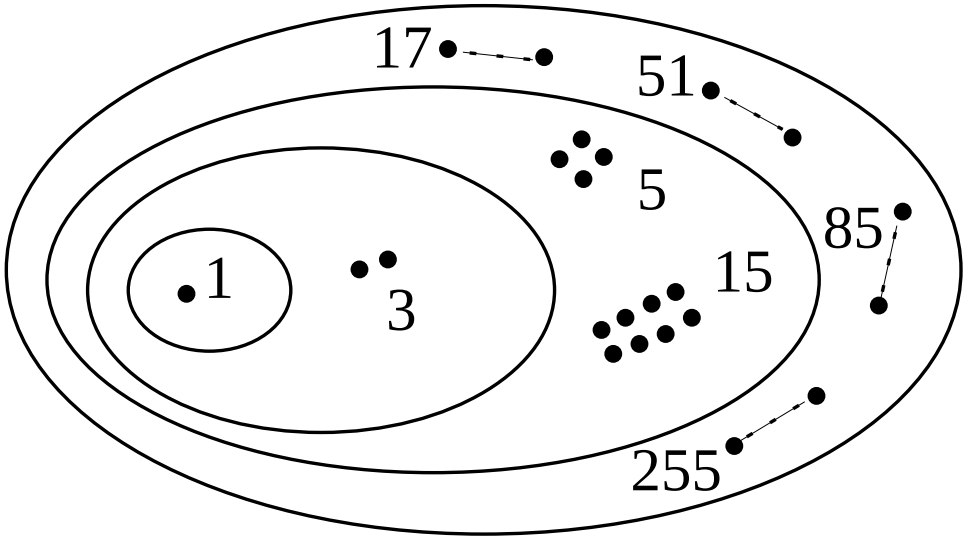
Rappel

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

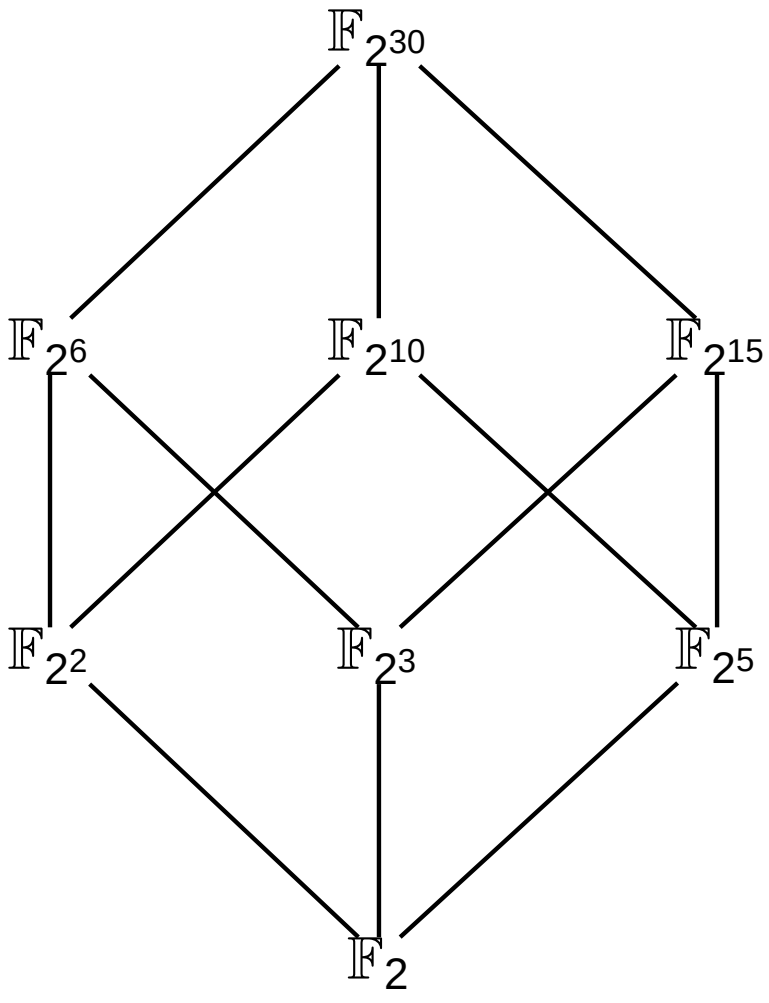
Dans ce tableau, il faut comprendre que tous les éléments repris dans les k premières lignes appartiennent aussi aux sous-champs apparaissant "plus bas" (à cause de l'emboîtement).

	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 $\mathbb{F}_q$



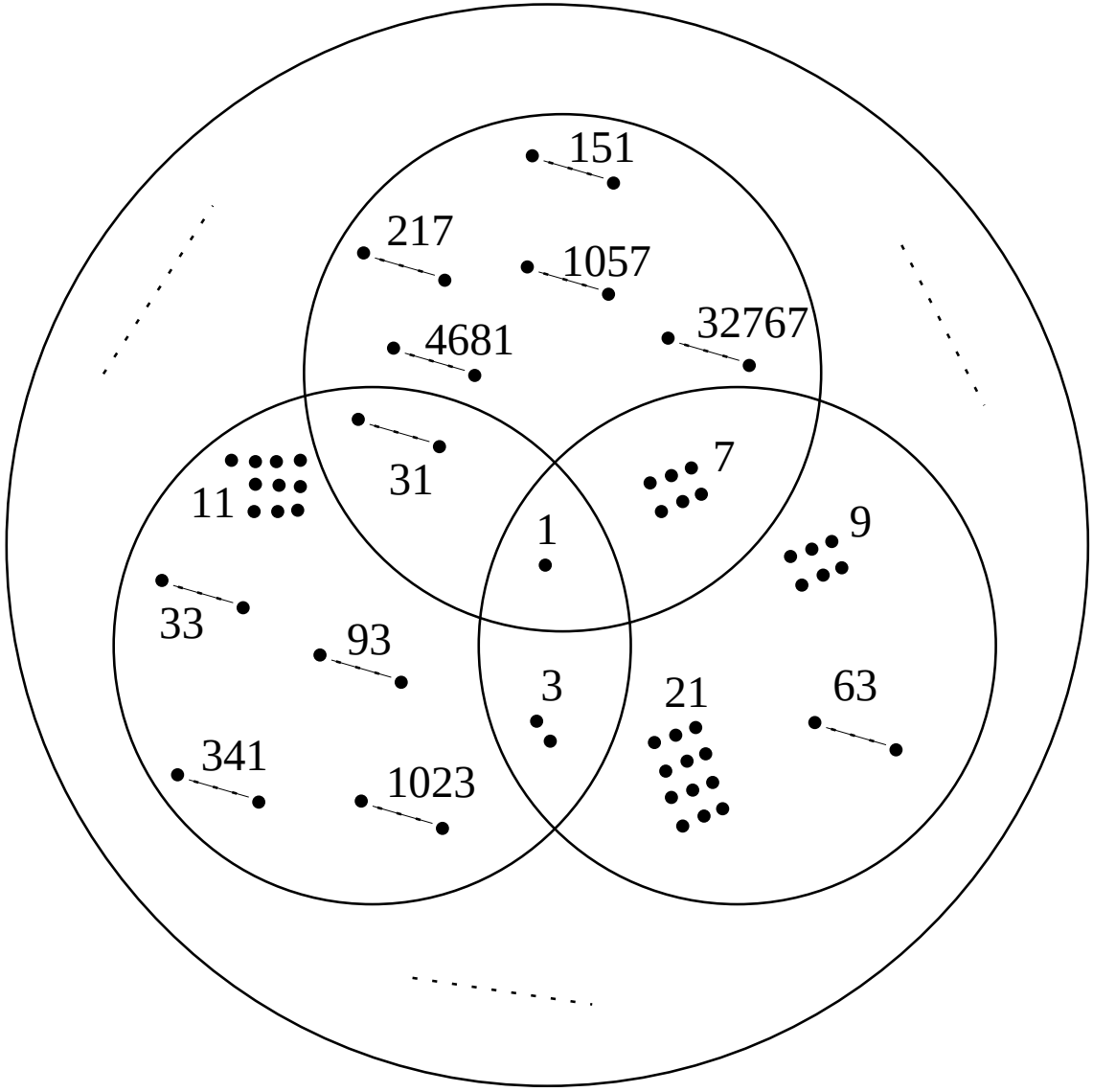
Sous-champs de $\mathbb{F}_q$

	ord	#	déjà pris en compte
$\mathbb{F}_2^*$	1	1	
$\mathbb{F}_{2^2}^*$			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	

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	
	$\vdots$	$\vdots$	
	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

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

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 $N_p(f)$... "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}
```

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 $\mathbb{F}_{p^s}[\alpha] = \mathbb{F}_{p^s}(\alpha) \tilde{=} \mathbb{F}_{p^s}[X]/\langle M_\alpha \rangle$ 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 $b \geq 2$

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

$\rho_b(n) = \sigma_{\ell-1} \cdots \sigma_0$: 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

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

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

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

- 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

$$
\begin{array}{cccccccccc}
 & & & & & 1 & 1 & 0 & 0 & 1 \\
\times & & & & & & 1 & 1 & 0 & 1 \\
\hline
 & & & & & 1 & 1 & 0 & 0 & 1 \\
 & & & 1 & 1 & 0 & 0 & 1 & & \\
+ & 1 & 1 & 0 & 0 & 1 & & & & \\
\hline
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1
\end{array}
$$

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 $a \neq 0$.

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

$\mathrm{pgcd}(a, b) = r_j$. 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

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

Complexité des opérations

Exemple

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

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

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

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

Complexité des opérations

L'algorithme d'Euclide étendu :
calcul simultané de $\mathrm{pgcd}(a, b)$ 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.

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

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 $r_1 = 9,\ r_2 = 4,\ r_3 = 1,\ r_4 = 0.$

$$A_0 = 0,\ A_1 = 1,\ A_2 = q_1 A_1 + A_0 = 6,$$
$$A_3 = q_2 A_2 + A_1 = 79,\ A_4 = q_3 A_3 + A_2 = 164,$$
$$B_0 = 1,\ B_1 = 0,\ B_2 = q_1 B_1 + B_0 = 1,$$
$$B_3 = q_2 B_2 + B_1 = 13,\ B_4 = q_3 B_3 + B_2 = 27.$$

De là, par la proposition précédente, il vient

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

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 :

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

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 !

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,

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

A PROPOS DES NOMBRES PREMIERS

REMARQUE

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

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

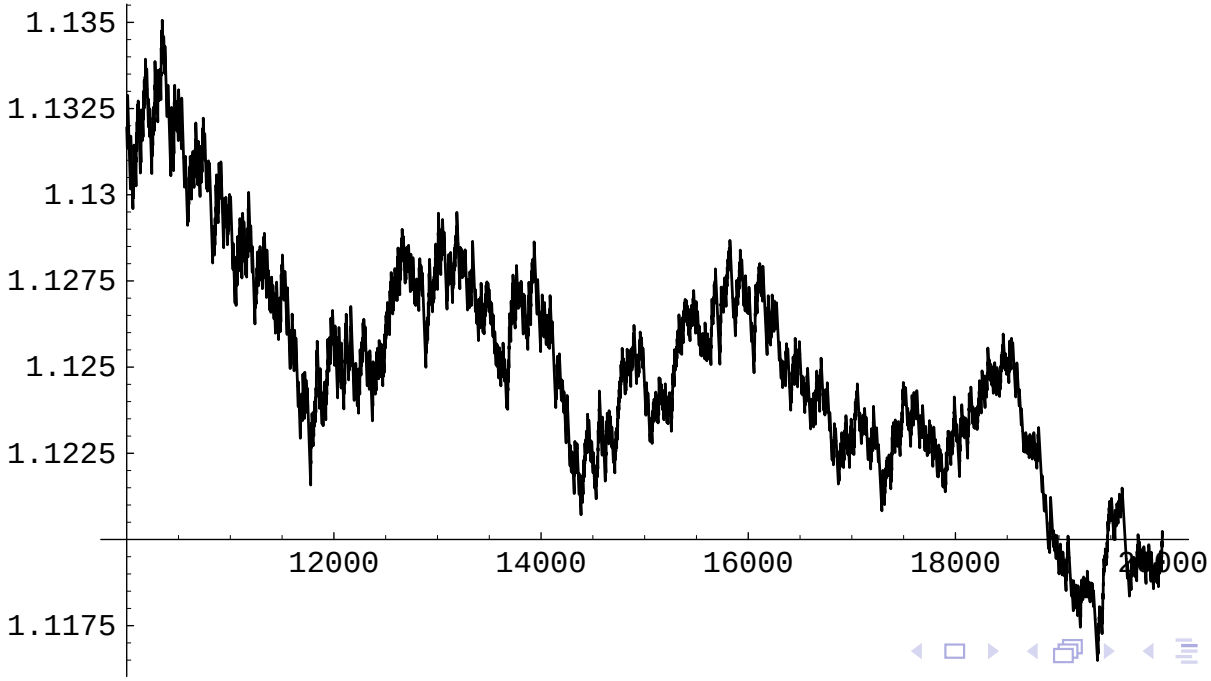
Par contre, il est conjecturé qu'il existe une infinité de nombres premiers jumeaux, i.e., tels que p et $p+2$ soient premiers.

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 $10^4 \leq n \leq 2.10^4$.



A PROPOS DES NOMBRES PREMIERS

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.