

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Bracelets de De Bruijn

Systèmes de Steiner

Divers

# Vendredi : Corps finis (suite)

## Cours de remise à niveau MPRI 2006–2007

David A. Madore  
david.madore@ens.fr

15 septembre 2006

# Programme du cours

- ▶ Lundi : Entiers ( $\mathbb{Z}$ )
- ▶ Mardi : Entiers modulaires ( $\mathbb{Z}/n\mathbb{Z}$ )
- ▶ Mercredi : Polynômes ( $k[t]$ )
- ▶ Jeudi : Corps finis ( $\mathbb{F}_q$ )
- ▶ Vendredi : Corps finis, suite ( $\mathbb{F}_q[t]$ )

9h30 à 12h00 ; salle OD4

Vendredi : Corps finis (suite)

David Madore

Programme du cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés distincts

L'algorithme de Cantor-Zassenhaus

Partage de secret

Quelques utilisations en combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

# Table des matières

## Rappels

## Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés distincts

L'algorithme de Cantor-Zassenhaus

## Partage de secret

## Quelques utilisations en combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

Vendredi : Corps  
finis (suite)

David Madore

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

# Rappels des épisodes précédents

- ▶ Le cardinal d'un corps fini est une puissance d'un nombre premier  $q = p^d$ .
- ▶ Pour tout  $q = p^d$ , il existe un corps fini ayant  $q$  éléments, unique à isomorphisme (non-unique) près.
- ▶  $\mathbb{F}_q = \{x : x^q = x\}$  (dans tout corps plus gros).
- ▶ On a  $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^{d'}}$  si et seulement si  $p = p'$  et  $d|d'$ .
- ▶  $\mathbb{F}_q^\times$  est cyclique (ses générateurs s'appellent éléments *primitifs*).
- ▶ Tout  $x \in \mathbb{F}_{q^e}$  est racine d'un unique polynôme unitaire irréductible sur  $\mathbb{F}_q$ , de degré divisant  $e$ , appelé son *polynôme minimal* : ses racines s'appellent les *conjugés* de  $x$  et sont les  $x^{q^i}$ .
- ▶  $t^{q^e} - t$  est le produit de tous les polynômes unitaires irréductibles de degré divisant  $e$ , un pour chaque classe de conjugaison.

# Test d'irréductibilité de Rabin (rappel)

Vendredi : Corps  
finis (suite)

David Madore

Programme du  
cours

Table des matières

Rappels

Factorisation

**Irréductibilité**

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

**Test de Rabin (1980)** : Donné un  $f \in \mathbb{F}_q[t]$  de degré  $e$ , comment savoir s'il est irréductible ? Il faut et il suffit qu'il vérifie chacune des deux conditions :

- ▶  $f$  est premier avec  $t^{q^{e_1}} - t$  pour tout diviseur strict  $e_1$  de  $e$ , et
- ▶  $f$  divise  $t^{q^e} - t$ .

Évidemment  $q^e$  et  $q^{e_1}$  peuvent être très grands, mais on calcule tout *modulo*  $f$  (c'est-à-dire dans  $\mathbb{F}_q[t]/(f)$ ), en utilisant l'écriture binaire de l'exposant  $q^e$  et l'élévation au carré successive, pour calculer le reste de la division de  $t^{q^e} - t$  par  $f$ , et de même pour  $q^{e_1}$ .

# Démonstration du test de Rabin

Si  $f \in \mathbb{F}_q[t]$  de degré  $e$  est irréductible, alors

- ▶ *toute* racine  $\xi$  de  $f$  (dans  $\overline{\mathbb{F}}$ ) est de degré  $e$  sur  $\mathbb{F}_q$  donc dans  $\mathbb{F}_{q^e}$ , donc  $\xi^{q^e} = \xi$ , donc  $f$  divise  $t^{q^e} - t$ ,
- ▶ *aucune* racine  $\xi$  de  $f$  n'est de degré  $e_1 < e$ , i.e., n'est racine de  $t^{q^{e_1}} - t$ .

Si  $f \in \mathbb{F}_q[t]$  de degré  $e$  vérifie les deux critères du test de Rabin, alors tout facteur irréductible de  $f$

- ▶ est de degré divisant  $e$  puisque  $f$  divise  $t^{q^e} - t$  (qui est produit de tous les irréductibles de degré divisant  $e$ ,
- ▶ ne peut pas être de degré  $e_1 < e$  d'après la seconde condition.

# Génération de polynômes irréductibles

Vendredi : Corps  
finis (suite)

David Madore

Pour trouver  $f$  irréductible de degré  $d$ , il suffit de répéter :

- ▶ tirer aléatoirement  $f$  unitaire de degré  $d$  dans  $\mathbb{F}_p[t]$ ,
- ▶ tester l'irréductibilité,

jusqu'à trouver  $f$  qui convient.

Le nombre d'essais à faire est statistiquement de l'ordre de  $d$ , car la proportion de polynômes de degré  $d$  irréductibles dans  $\mathbb{F}_q[t]$  est environ  $\frac{1}{d}$ .

(Leur nombre exact est  $\frac{1}{d}(q^d - \sum_{\ell} q^{d/\ell} + \sum_{\ell_1 \neq \ell_2} q^{d/\ell_1 \ell_2} - \dots)$ , avec  $\ell_i$  les facteurs premiers de  $d$ .)

**Test de Ben-Or :** Calculer  $\text{pgcd}(f, t^{q^i} - t)$  pour  $i = 1, \dots, \lfloor \frac{d}{2} \rfloor$  et s'arrêter ( $f$  n'est pas irréductible) si jamais un p.g.c.d. n'est pas 1.

(Plus rapide que le test de Rabin, pour la génération, car le degré du plus petit facteur irréductible est « petit » (en  $O(\log d)$ ).

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

On dit que  $f \in \mathbb{F}_q[t]$  est **sans facteur carré** ssi (conditions équivalentes) :

- ▶ toutes les racines de  $f$  dans  $\overline{\mathbb{F}}$  sont simples,
- ▶ dans la décomposition de  $f$  en facteurs irréductibles,  $c \prod_h h^{v_h(f)}$ , toutes les multiplicités  $v_h(f)$  valent 1,
- ▶  $\text{pgcd}(f, f') = 1$ ,
- ▶  $\mathbb{F}_q[t]/(f)$  est un produit de corps.

Si  $f = \prod_h h^{v_h(f)}$  (mettons unitaire) est une décomposition en irréductibles, **la partie sans facteur carré** de  $f$  est par définition  $\prod_{h: v_h(f) > 0} h$  (le plus grand polynôme sans facteur carré divisant  $f$ ).

# Calcul de la partie sans facteur carré

Vendredi : Corps  
finis (suite)

David Madore

Soit  $f = \prod_i h_i^{v_i}$  avec  $h_i$  irréductibles (distincts) : on cherche à calculer la partie sans facteur carré de  $f$ .

- ▶ si  $g = \text{pgcd}(f, f')$ , on montre que  $f/g = \prod h_i$ , le produit étant pris sur les  $h_i$  tels que  $p \nmid v_i$  (le plus souvent, cela suffit !),
- ▶ dans ce cas,  $f/\text{pgcd}(f, (f/g)^N)$  avec  $N$  grand (par exemple  $N = \deg f$ ), ou, mieux,  $g/\text{pgcd}(g, (f/g)^N)$ , vaut  $\prod h_i^{v_i}$  sur les  $i$  tels que  $p \mid v_i$ ,
- ▶ c'est donc une puissance de  $p$ , et il est facile de calculer sa racine  $p$ -ième,
- ▶ ...et on continue ainsi.

On pourra donc se ramener à factoriser des polynômes sans facteur carré.

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

**Partie sans facteur carré**

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

# Décomposition en degrés distincts

Vendredi : Corps  
finis (suite)

David Madore

Rappel :  $t^{q^d} - t$  est le produit de tous les polynômes irréductibles de degré divisant  $d$  (chacun apparaissant avec multiplicité 1).

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

On suppose  $f_1 = f$  sans facteur carré :

- ▶ on calcule successivement  $f_{i+1} = f_i / \text{pgcd}(f_i, t^{q^i} - t)$  (jusqu'à tomber sur  $f_i = 1$ ),
- ▶ les  $g_i = \text{pgcd}(f_i, t^{q^i} - t)$  calculés successivement sont justement les produits des facteurs irréductibles de degré  $i$  de  $f$ ,
- ▶ il suffira de factoriser chacun,
- ▶ si  $\deg g_i = i$ , on sait déjà que  $g_i$  est irréductible,
- ▶ on peut s'arrêter dès que  $\deg f_i < 2i$  (alors  $f_i$  est irréductible puisque chaque facteur irréductible doit être de degré au moins  $i$ ).

Le plus souvent, ceci suffit à factoriser complètement  $f$  !

# Factorisation en degrés égaux (problème)

Vendredi : Corps  
finis (suite)

David Madore

On cherche maintenant à factoriser  $f = \prod_{i=1}^{i=r} h_i$ , où les  $h_i$  sont irréductibles, distincts, de même degré  $d$ .

Il suffit de trouver une factorisation non triviale  $f = f_1 f_2$  (on pourra alors répéter l'opération pour  $f_1$  et  $f_2$ ).

D'après le théorème chinois, on a  $\mathbb{F}_q[t]/(f) \cong \prod_{i=1}^{i=r} \mathbb{F}_{q^d}$  :

- ▶ si  $a \in \mathbb{F}_q[t]/(f)$ , on note  $(a_1, \dots, a_r)$  ses composantes par cet isomorphisme,
- ▶ comme les  $h_i$  sont inconnus, on ne sait pas calculer les  $a_i$ ,
- ▶ en revanche, on sait tester si certains sont nuls, car alors  $\text{pgcd}(f, a) \neq 1$ ,
- ▶ et c'est ce qu'on cherche à obtenir.

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

# Factorisation en degrés égaux (carac. $\neq 2$ )

On cherche à factoriser  $f = \prod_{i=1}^{i=r} h_i$ , où les  $h_i$  sont irréductibles, distincts, de même degré  $d$ .

## Algorithme de Cantor-Zassenhaus (cas $p$ impair) :

- ▶ tirer  $a \in \mathbb{F}_q[t]/(f)$  au hasard (recommencer tant que  $a = 0$ ),
- ▶ si  $\text{pgcd}(f, a) \neq 1$ , fini (on a trouvé une factorisation non triviale),
- ▶ sinon, calculer  $b = a^{(q^d-1)/2}$  (modulo  $f$ ) : comme toutes les composantes  $a_i$  sont non nulles, toutes les  $b_i$  valent  $\pm 1$ ,
- ▶ si  $b = \pm 1$ , recommencer,
- ▶ sinon,  $\text{pgcd}(f, b - 1)$  donne une factorisation non triviale.

On utilise le fait que  $x^{(q^d-1)/2} = \pm 1$  pour tout  $x \in \mathbb{F}_{q^d}^\times$ , avec la valeur  $+$  pour la moitié d'entre eux (ceux qui sont des carrés), et  $-$  pour l'autre moitié.

# Factorisation en degrés égaux (carac. 2)

Vendredi : Corps  
finis (suite)

David Madore

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

On cherche à factoriser  $f = \prod_{i=1}^{i=r} h_i$ , où les  $h_i$  sont irréductibles, distincts, de même degré  $d$ .

**Algorithme de Cantor-Zassenhaus** (cas  $p = 2$ ) :

- ▶ tirer  $a \in \mathbb{F}_q[t]/(f)$  au hasard,
- ▶ calculer  $b = a + a^2 + a^4 + \dots + a^{q^d/2}$  : toutes les  $b_i$  valent 0 ou 1,
- ▶ si  $b = 0$  ou  $b = 1$ , recommencer,
- ▶ sinon,  $\text{pgcd}(f, b)$  donne une factorisation non triviale.

On utilise le fait que  $x + x^2 + x^4 + \dots + x^{q^d/2} \in \{0, 1\}$  pour tout  $x \in \mathbb{F}_{q^d}$ , avec la valeur 0 pour la moitié d'entre eux (ceux qui sont de la forme  $z^2 + z$  avec  $z \in \mathbb{F}_{q^d}$ ), et 1 pour l'autre moitié.

# Principe du partage de secret

Vendredi : Corps  
finis (suite)

David Madore

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

Alice possède un secret  $M$  et veut le partager en  $M_1, \dots, M_r$  parts telles que :

- ▶ la connaissance de  $\geq s$  parts quelconques permet de reconstituer  $M$ ,
- ▶ la connaissance de  $< s$  parts n'apporte *aucune information* sur  $M$  (sauf éventuellement sa longueur).

# Utilisation du polynôme interpolateur

Vendredi : Corps  
finis (suite)

David Madore

Pour un corps fini  $\mathbb{F}_q$  convenable : on supposera  $M \in \mathbb{F}_q$  (quitte à couper  $M$  en plusieurs blocs).

Méthode de partage de secret en  $r$  parts telles que  $s$  suffisent à reconstituer :

- ▶ on convient de valeurs  $a_0, a_1, \dots, a_r \in \mathbb{F}_q$  (deux à deux distinctes),
- ▶ on tire au hasard  $M_1, \dots, M_{s-1} \in \mathbb{F}_q$  (uniformément),
- ▶ on calcule l'unique  $f \in \mathbb{F}_q[t]$  de degré  $< s$  tel que  $f(a_0) = M$  et  $f(a_i) = M_i$  (pour chaque  $i = 1, \dots, s - 1$ ),
- ▶ les parts sont les  $M_1 = f(a_1), \dots, M_r = f(a_r)$ ,
- ▶ la connaissance de  $\geq s$  d'entre elles permet de retrouver  $f$  donc  $f(a_0) = M$ .

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

On veut adjoindre à chaque lot de  $s$  blocs du message un ensemble de  $r - s$  blocs correcteurs d'erreur, de sorte que connaître  $s$  parmi les  $r$  blocs suffise à retrouver les blocs initiaux :

- ▶ cette fois,  $M_1, \dots, M_s$  sont des blocs du message,
- ▶ on calcule encore  $f$  de degré  $< s$  tel que  $f(a_i) = M_i$  pour  $i = 1, \dots, s$ ,
- ▶ les parts sont les  $M_i = f(a_i)$  pour  $i = 1, \dots, r$ ,
- ▶ la connaissance de  $\geq s$  d'entre elles permet de retrouver  $f$  donc tous les  $f(a_i) = M_i$  (pour  $i = 1, \dots, r$ ), notamment ceux du message d'origine.

On appelle **bracelet de De Bruijn** d'ordre  $d$  sur un alphabet  $S$  à  $q$  lettres une application  $b: \mathbb{Z}/q^d\mathbb{Z} \rightarrow S$  telle que chaque  $d$ -uplet  $w \in S^d$  apparaisse à un emplacement dans le bracelet, i.e., il existe  $o$  tel que  $b(o+i) = w(i)$  pour  $i = 0, \dots, d-1$ .

**Exemple** : 0000100110101111 est un bracelet de De Bruijn d'ordre 4 sur un alphabet à deux lettres.

00000100101100111110001101110101 en est un d'ordre 5.

Si  $q = p^e$ , on peut construire un bracelet de De Bruijn d'ordre  $d$  sur un alphabet à  $q$  lettres de la façon suivante :

- ▶ soit  $g \in \mathbb{F}_{q^d}^\times$  primitif (donc d'ordre  $q^d - 1$ ),
- ▶ on écrit chaque puissance  $g^i$  de  $g$  sur la base  $1, g, g^2, \dots, g^{d-1}$  de  $\mathbb{F}_{q^d}$  sur  $\mathbb{F}_q$ ,
- ▶ si  $b(i)$  est le coefficient sur 1 de  $g^i$ , alors  $b: \mathbb{Z}/(q^d - 1)\mathbb{Z} \rightarrow \mathbb{F}_q$  fournit un « presque » bracelet de De Bruijn, auquel il ne manque que le  $0 \dots 0$  (de longueur  $d$ ),
- ▶ en insérant un 0 supplémentaire dans une suite de 0 de longueur  $d - 1$ , on obtient un bracelet de De Bruijn.

**Exercice :** Expliquer comment obtenir un bracelet de De Bruijn si  $q$  n'est pas une puissance d'un nombre premier.

On appelle **système de Steiner** d'indices  $(\ell, m, n)$

- ▶ un ensemble de  $n$  « points » parmi lesquels
- ▶ des « blocs » de  $m$  points ont été définis de telle sorte que
- ▶ chaque ensemble de  $\ell$  points soit inclus dans un et un seul bloc.

Le nombre de blocs est nécessairement  $C_n^\ell / C_m^\ell$  (il faut donc qu'il soit entier).

En général, il est très difficile de déterminer s'il existe un système de Steiner d'indices  $(\ell, m, n)$  donnés et, lorsqu'il existe, s'il est unique.

Exemple : il existe un système de Steiner d'indices  $(5, 8, 24)$ , qui est un des objets combinatoires les plus remarquables qui soient.

On appelle **plan affine**  $\mathbb{A}_{\mathbb{F}_q}^2$  sur le corps fini  $\mathbb{F}_q$  l'ensemble  $\mathbb{F}_q^2$  muni de parties à  $q$  éléments appelées *droites* : si  $(x_0, y_0) \in \mathbb{F}_q^2$  et  $(u, v) \neq 0$ , la droite passant par  $(x_0, y_0)$  dirigée par  $(u, v)$  est donnée par

$$\{(x_0 + tu, y_0 + tv) : t \in \mathbb{F}_q\}$$

Chaque droite contient  $q$  points, et chaque paire de points (distincts !) appartient à une et une seule droite, autrement dit :

- ▶  $\mathbb{A}_{\mathbb{F}_q}^2$  forme un système de Steiner d'indices  $(2, q, q^2)$ .

On appelle **plan projectif**  $\mathbb{P}_{\mathbb{F}_q}^2$  sur le corps fini  $\mathbb{F}_q$  l'ensemble des triplets  $(x, y, z) \in \mathbb{F}_q^3 \setminus \{(0, 0, 0)\}$  quotienté par la relation d'équivalence  $(x, y, z) \sim (tx, ty, tz)$  pour tout  $t \in \mathbb{F}_q^\times$ .

On note  $(x : y : z)$  la classe d'équivalence de  $(x, y, z)$ .

Si  $(x : y : z) \neq (x' : y' : z')$ , on appelle *droite (projective)* passant par ces points l'ensemble

$$\{(\lambda x + \mu x' : \lambda y + \mu y' : \lambda z + \mu z')\}$$

Le plan projectif a  $q^2 + q + 1$  points, chaque droite projective en contient  $q + 1$ , et chaque paire de points (distincts) appartient à une et une seule droite, autrement dit :

- ▶  $\mathbb{P}_{\mathbb{F}_q}^2$  forme un système de Steiner d'indices  $(2, q + 1, q^2 + q + 1)$ .

Si  $Q \in \mathbb{F}_q[x, y, z]$  est un polynôme homogène de degré 2 non nul et irréductible, la **conique** associée dans  $\mathbb{P}_{\mathbb{F}_q}^2$  est par définition

$$C_Q = \{(x : y : z) : Q(x, y, z) = 0\}$$

elle a toujours exactement  $q + 1$  points.

On dit qu'une droite  $d$  est *tangente* à la conique  $C$  lorsque  $d$  rencontre  $C$  en exactement un point.

Par chaque point de la conique passe exactement une droite tangente.

Si  $C \subset \mathbb{P}_{\mathbb{F}_q}^2$  est une conique, il existe une unique bijection

$$\{\text{points de } \mathbb{P}_{\mathbb{F}_q}^2\} \leftrightarrow \{\text{droites de } \mathbb{P}_{\mathbb{F}_q}^2\}$$

qui préserve l'incidence et envoie chaque point de la conique sur la droite tangente en ce point.

(Moralité : les points et les droites du plan projectif jouent des rôles complètement symétriques.)

Une **matrice d'Hadamard** de taille  $n$  (nécessairement paire) est une matrice  $M \in \mathbb{M}_n(\mathbb{R})$  à coefficients dans  $\{\pm 1\}$  telle que  $M^t M = nI_n$ , autrement dit :

- ▶ deux rangées différentes quelconques de  $M$  ont le même signe sur  $n/2$  colonnes et des signes différents sur les  $n/2$  autres.

On conjecture qu'il existe une matrice d'Hadamard pour toute taille  $n$  multiple de 4.

Exemple : matrice d'Hadamard de taille 4 :

$$\begin{pmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & -1 & +1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & +1 & -1 \end{pmatrix}$$

Si  $q$  est une puissance d'un nombre premier et  $q \equiv 3 \pmod{4}$ , on construit une matrice d'Hadamard de taille  $q + 1$  grâce à la fonction  $\varphi: \mathbb{P}_{\mathbb{F}_q}^1 \times \mathbb{P}_{\mathbb{F}_q}^1 \rightarrow \{\pm 1\}$  (où  $\mathbb{P}_{\mathbb{F}_q}^1 = \mathbb{F}_q \cup \{\infty\}$ ) définie par

$$\begin{aligned}\varphi(\infty, \infty) &= \varphi(x, \infty) = \varphi(\infty, y) = +1 \\ \varphi(x, x) &= -1 \\ \varphi(x, y) &= (x - y)^{(q-1)/2} \text{ si } x \neq y\end{aligned}$$

(Rappel : pour  $t \in \mathbb{F}_q^\times$ , on a  $t^{(q-1)/2} \in \{\pm 1\}$ , la valeur  $+1$  étant prise si et seulement si  $t$  est un carré.)

# Un problème combinatoire

Vendredi : Corps  
finis (suite)

David Madore

Programme du  
cours

Table des matières

Rappels

Factorisation

Irréductibilité

Partie sans facteur carré

Décomposition en degrés  
distincts

L'algorithme de  
Cantor-Zassenhaus

Partage de secret

Quelques  
utilisations en  
combinatoire

Bracelets de De Bruijn

Systèmes de Steiner

Divers

On considère le problème suivant :  $q = p^d$  joueurs veulent jouer à un jeu qui se déroule en plusieurs manches : on veut que

- ▶ chaque joueur arbitre (et ne joue pas) pendant une et une seule manche (il y aura donc  $q$  manches),
- ▶ les joueurs non arbitres jouent de manière cyclique,
- ▶ sur les  $q - 1$  manches où il joue, chaque joueur aura une et une seule fois chaque autre joueur comme joueur suivant.

**Exercice** : Comment résoudre ce problème avec les corps finis ?