123 CORPS FINIS. APPLICATIONS.

Cadre : un corps est par définition un anneau commutatif non nul A tel que $A^\times = A \setminus \{0\}$

Il est dit fini lorsque son cardinal est fini.

I / Structures autour des corps finis

Rq 1 . Il existe des corps finis. En effet

Prop 2 p est premier $\Leftrightarrow$ $\mathbb{Z}/p\mathbb{Z}$ est intègre $\Leftrightarrow$ $\mathbb{Z}/p\mathbb{Z}$ est un corps

Dans la suite de la partie I, K désigne un corps fini.

1) Caractéristique et cardinal

Prop 3 . $\varphi : \mathbb{Z} \longrightarrow K$, $k \mapsto k.1$ est un morphisme d'anneaux de noyau $p\mathbb{Z}$. p est un nombre premier

Def 4 On nomme "caractéristique de K", noté car(K), l'entier p

Rq 5 $\mathbb{Z}/p\mathbb{Z}$ est le sous corps premier de K.

Prop 6 K est un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel de dimension finie.

Cor 7 : Il existe $n \geq 1$ tel que $\# K = p^n$

Ex 8 : Il n'existe pas de corps à 6 éléments.

2) Structure du groupe des inversibles $K^\times$

Prop 9 . $K^\times$ est cyclique. $K^\times \simeq \mathbb{Z}/(p^n-1)\mathbb{Z}$

Rq 10 : En fait, tout sous groupe de $K^\times$ est cyclique

Rq 10 . Plus généralement, tout sous groupe fini de $L^\times$ pour L, corps quelconque (même infini) est cyclique.

Ex 11 . $(\mathbb{Z}/7\mathbb{Z})^\times$ est cyclique engendré par 3.

3) Automorphismes de K

Prop 12 . $\varphi : K \longrightarrow K$, $x \mapsto x^p$ est un automorphisme de K. [DEM] p211

Def 12 . Ce morphisme est nommé morphisme de Frobenius.

Rq 13 . Si $K = \mathbb{Z}/p\mathbb{Z}$, le petit théorème de Fermat assure que φ = identité

Prop 14 . La condition $x^p = x$ équivaut à $x \in \mathbb{Z}/p\mathbb{Z}$

Si $Q \in K[X]$, $Q(X^p) = Q(X)^p$ ssi les coefficients de Q sont dans $\mathbb{Z}/p\mathbb{Z}$

Prop 15 . Soit $\alpha \in K$ et n le degré de α sur $\mathbb{Z}/p\mathbb{Z}$. Alors n est le plus petit entier tel que $\alpha^{p^n} = \alpha$ et le polynôme minimal de α sur $\mathbb{Z}/p\mathbb{Z}$ est $(X-\alpha)(X-\alpha^p)\dots(X-\alpha^{p^{n-1}})$.

Prop 16 Soit f un automorphisme de K. Alors il existe $s \geq 0$ tel que pour tout $x \in K$, $f(x) = x^{p^s}$

Cor 17 . $\mathrm{Aut}(K) = \langle \varphi \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

4) Existence, unicité, sous corps d'un corps fini

Th 18 Pour tout p premier et tout $n \geq 1$, il existe un corps de cardinal p^n. Il est unique à isomorphisme près et on le note $\mathbb{F}_{p^n}$. [DEM] p223

Rq 19 . Cet isomorphisme n'est en revanche pas unique

Prop 20 . $\forall n \geq 1$, $\forall p$ premier, il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$ (le polynôme minimal d'un générateur de $\mathbb{F}_{p^n}^\times$ convient par exemple). On peut donc construire $\mathbb{F}_{p^n}$ comme quotient de $\mathbb{F}_p[X]$ par un tel polynôme irréductible.

Ex 21 X^2+X-1 est irréductible dans $\mathbb{F}_3[X]$ donc $\mathbb{F}_9 \simeq \dfrac{\mathbb{F}_3[X]}{(X^2+X-1)}$

[PCR] p77
[PER] p78
[PER] p78
[EA1]

Prop 22. $\mathbb{F}_{p^d}$ est un sous corps de $\mathbb{F}_{p^n}$ ssi $d \mid n$.
Dans ce cas, $\mathbb{F}_{p^d}$ est l'ensemble des points fixes de φ^d où $\varphi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ est le Frobenius

Ex 23 Les sous corps de $\mathbb{F}_{16}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_{16}$.

Prop 24 $\bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de tout corps fini de caractéristique p.

II / Polynômes sur les corps finis

1) Polynômes irréductibles sur $\mathbb{F}_q$, $q = p^n$

Prop 24+½ Soit $Q = \sum_{i=1}^{m} a_i X^i \in \mathbb{Z}[X]$ et p premier. Si $\bar{Q} = \sum_{i=1}^{m} \bar{a_i} X^i$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ et $\deg(Q) = \deg(\bar{Q})$ alors Q est irréductible dans $\mathbb{Z}[X]$.
Connaître les polynômes irréductibles de $\mathbb{F}_p[X]$ peut montrer l'irréductibilité dans $\mathbb{Z}[X]$

Ex 25 $P = 3X^3 + 7X + 1$ est irréductible dans $\mathbb{Z}[X]$ (et dans $\mathbb{Q}[X]$) car en réduisant modulo 2, on a $\deg(P) = \deg(\bar{P})$ et $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.

Ct. ex 26 : $X^4 + 1$ est irréductible sur $\mathbb{Z}$ mais est réductible sur $\mathbb{F}_p$ pour tout premier p.

Prop 27 Soit $P \in k[X]$ de degré n. P est irréductible sur k $\iff$ P n'a pas de racines dans les extensions K de k telles que $[K:k] \leq \frac{n}{2}$.

Ex 28 $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2$.

Th 29 Pour $d \geq 1$, on note $P_d = \{$polynômes irréductibles de degré d dans $\mathbb{F}_q[X]\}$ Alors $X^{q^n} - X = \prod_{d \mid n} \prod_{P \in P_d} P$, pour tout $n \in \mathbb{N}^*$

Prop 30 $\# P_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$ où μ est la fonction de Möbius

[DA] p245
[SER] p12

Prop 31 Critère d'irréductibilité de Rabin. Soit $P \in \mathbb{F}_q[X]$ unitaire et de degré n.
P est irréductible sur $\mathbb{F}_q$ $\iff$ $\begin{cases} P \mid X^{(q^n)} - X \\ \text{pour tout facteur premier } l \text{ de } n, \\ \text{Pgcd}(P, X^{(q^{n/l})} - X) = 1. \end{cases}$

2) Algorithme de factorisation de Berlekamp

Algo 32. Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés et notons $x = X \bmod P$ dans $\mathbb{F}_q[X]/(P)$.
Entrée de l'algorithme : P. Sortie = les facteurs irréductibles $P_1, \dots, P_r$ de P ($P = P_1 \times \dots \times P_r$). Déroulement :

① Calculer dans la base $(1, x, \dots x^{\deg(P)-1})$ la matrice de $S_P - \mathrm{Id}$ où $S_P : Q \in \mathbb{F}_q[X]/(P) \longmapsto Q^q \bmod P$.

② Calculer $\dim(\mathrm{Ker}(S_P - \mathrm{Id}))$. Elle vaut r. Si $r = 1$, P est irréductible et on s'arrête, sinon

③ Calculer $V \in \mathrm{Ker}(S_P - \mathrm{Id})$ non constant modulo P.
Alors $P = \prod_{a \in \mathbb{F}_q} \mathrm{pgcd}(P, V - a)$ et parmi ces facteurs, au moins un n'est pas trivial. On réapplique l'algorithme à tous les facteurs non triviaux de ce produit. DEV 1

3) Équations sur un corps fini $\mathbb{F}_q$ où $q = p^s$.

Th 33 (Chevalley - Warning)
Soit $n, r \in \mathbb{N}^*$ et $f_1, \dots f_r \in \mathbb{F}_q[X_1, \dots X_n]$ tels que $\sum_{i=1}^{r} \deg(f_i) < n$
Notons $Z = \{x \in \mathbb{F}_q^n \mid \forall i \in [\![1, r]\!], f_i(x) = 0\}$.
Alors $\# Z \equiv 0 \bmod p$ DEV 2

cor 34 Sous les mêmes hypothèses que th33, si les f_i sont sans terme constant alors ces polynômes admettent un zéro non trivial.

III/ Corps finis et arithmétique.

1) Critères de primalité

prop 35 Critère de Fermat et de Miller-Rabin.

Soit $n \in \mathbb{N}$. Si $\exists\, a \in [\![1, n]\!]$ tel que $a^{n-1} \not\equiv 1\ (n)$ alors n n'est pas premier. (critère de Fermat).

Plus précisément, si $\exists\, a \in [\![1, n]\!]$ et $\exists\, k \geq 0$ tels que $2^{k+1} \mid n-1$ et $a^{n-1} \equiv a^{\frac{n-1}{2}} \equiv \dots \equiv a^{\frac{n-1}{2^k}} \equiv 1 (n)$ et $a^{\frac{n-1}{2^{k+1}}} \not\equiv \pm 1 (n)$ alors n n'est pas premier.

[DEM] 76 prop 36 Soit $n \in \mathbb{N}^*$ impair. On suppose qu'on connaît les facteurs premiers de $n-1$. Alors n est premier $\Leftrightarrow$ $\exists\, a \in \mathbb{N}$ tel que $a^{n-1} \equiv 1 (n)$ et $a^{\frac{n-1}{q}} \not\equiv 1 (n)$ pour tout q facteur premier de $n-1$

2) Carrés dans $\mathbb{F}_p$ pour p premier

Rq 37. Tout élément de $\mathbb{F}_{2^n}$ est un carré car le Frobenius sur $\mathbb{F}_{2^n}$ est un automorphisme (car l'élévation au carré est le Frobenius)

Dans la suite, p est un premier impair

def 38 Symbole de Legendre.

Soit $a \in \mathbb{Z}$. $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0\ (p) \\ 1 \text{ si } a \text{ est un carré non nul modulo } p \\ -1 \text{ sinon.} \end{cases}$

prop 39 $\forall a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ (p)$

prop 40 pour tous $a, b \in \mathbb{Z}$, on a :

$a \equiv b\ (p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ et $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

cor 41 (découle de la prop 39) -1 est un carré mod p $\Leftrightarrow$ $p \equiv 1\ (4)$

appli 42 Il y a une infinité de nombres premiers congrus à 1 mod 4 [PER] p76

prop 43 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Autrement dit, 2 est un carré modulo p $\Leftrightarrow$ $p \equiv \pm 1\ (8)$

Th 44 Réciprocité quadratique.

Soit p, q premiers et impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$

Donc $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ sauf si p et q sont congrus à -1 modulo 4 ; auquel cas, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Ex 45 $\left(\frac{3}{7}\right) = -1$ donc 3 n'est pas un carré modulo 7

Prop 46 Soit p premier tq $p \equiv 3 (4)$. Si $\left(\frac{a}{p}\right) = 1$ alors $a^{\frac{p+1}{4}}$ est une racine carrée de a.

3) Ouverture cryptographique.

prop 47 Idée du protocole d'identification de Fiat-Shamir [BCS] p457

Soit $n = pq$ le produit de 2 grands entiers premiers. Alice est seule détentrice des identifiants $s_1, \dots, s_k$. Pour s'identifier à Bob, Alice lui envoie les $v_i = s_i^2$ mod n et $t = r^2$ mod n. Bob envoie alors $a_1, \dots a_k \in \{0,1\}^k$ à Alice. Alice calcule alors $y = r s_1^{a_1} \dots s_k^{a_k}$ mod n. Puis Bob vérifie que $y^2 \equiv t\, v_1^{a_1} \dots v_k^{a_k} (n)$. Il est difficile pour quelqu'un d'autre qu'Alice de s'authentifier car il faut pour cela connaître les racines carrées des v_i modulo n (difficile)

prop 48 Idée du cryptosystème de ElGamal [IHC] p 68

Soit G un groupe cyclique et g un générateur d'ordre q connu de tous. Alice choisit $x \in [\![1, q-1]\!]$ et calcule $h = g^x$ qu'elle diffuse. Pour lui envoyer un message, Bob choisit k au hasard dans $[\![1, q-1]\!]$ calcule $c_1 = g^k$ et $c_2 = h^k m$ où m est son message. Alice retrouve m en calculant $(c_1^x)^{-1} c_2$. Pour un autre qu'Alice ce problème est difficile dès lors que le problème du logarithme discret dans G est dur. C'est le cas dans certains $(\mathbb{F}_{p^n})^\times$

BIBLIOGRAPHIE

VLADISLAV TEMPEZ, AUDE LE GLUHER

— [PER] Daniel Perrin - Cours d'Algèbre.
— [DEM] Michel Demazure - Cours d'Algèbre : Primalité. Divisibilité. Codes.
— [SER] Jean-Pierre Serre - Cours d'Arithmétique.
— [OA] Jérôme Malick, Gabriel Peyré, Vincent Beck - Objectif Agrégation
— [EAL1] Serge Francinou, Hervé Gianella - Exercices de mathématiques pour l'agrégation : algèbre 1
— [IMC] Jeffrey Hoffsteini, Jill Pipher,Joseph H. Silverman - An Introduction to Mathematical Cryptography
— [ECS] Henk C.A. van Tilborg, Sushil Jajodia - Encyclopedia of Cryptography and Security

ALGORITHME DE BERLEKAMP

Référence : Objectif agrégation, Vincent Beck, Jérôme Malick, Gabriel Peyré, page 245

Théorème : Soit p un nombre premier et $q = p^s$ une puissance de p. Soit $P \in \mathbf{F}_q[X]$ dont la décomposition en facteurs irréductibles est sans facteurs carrés. Notons $x = X \bmod P$ dans l'anneau $\mathbf{F}_q[X]/(P)$. La famille $B = (1, x, \dots, x^{\deg(P)-1})$ est alors une base de $\mathbf{F}_q[X]/(P)$. En suivant les étapes suivantes (algorithme de Berlekamp), on obtient la décomposition en facteurs irréductibles de P :

on a un fac… pgcd(P, P') … P

(1) On observe que l'application $S_P : \left\{ \begin{array}{ccc} \mathbf{F}_q[X]/(P) & \longrightarrow & \mathbf{F}_q[X]/(P) \\ Q \bmod P & \longmapsto & Q^q \bmod P \end{array} \right.$ est linéaire. On calcule la matrice de $S_P - Id$ dans la base B.

(2) Le nombre de facteurs irréductibles de P, noté r, est égal à la dimension de $\mathrm{Ker}(S_P - Id)$. On calcule donc ce noyau par pivot de Gauss. Si $r = 1$ alors P est irréductible et on a terminé. Sinon, on passe à l'étape suivante.

(3) On choisit un polynôme V non constant dans $\mathbf{F}_q[X]/(P)$ et tel que $V \in \mathrm{Ker}(S_p - Id)$. On calcule ensuite avec l'algorithme d'Euclide tous les $\mathrm{pgcd}(P, V - a)$ pour a décrivant $\mathbf{F}_q$.

On a alors l'égalité $P = \prod_{a \in \mathbf{F}_q} \mathrm{pgcd}(P, V - a)$. On réapplique alors les étapes précédentes à tous les facteurs non triviaux (et il y en a) intervenant dans ce produit.

Démonstration : On montre la correction et la terminaison de cet algorithme.

(1) L'application S_P est bien $\mathbf{F}_q$-linéaire : on peux le montrer pédestrement un peu de la même façon qu'on montre que le morphisme de Frobenius en est bien un.

(2) On sait que $P = \prod_{i=1}^{r} P_i$ avec les P_i irréductibles et distincts, puisque P est sans facteur carré, et r le nombre de polynômes irréductibles constituant P. Les P_i sont deux à deux premiers entre eux ce qui autorise l'utilisation du théorème chinois. Ce dernier affirme l'existence d'un isomorphisme de $\mathbf{F}_q$-algèbres

$$\varphi : \left\{ \begin{array}{ccc} \mathbf{F}_q[X]/(P) & \longrightarrow & \mathbf{F}_q[X]/(P_1) \times \cdots \times \mathbf{F}_q[X]/(P_r) \\ Q \bmod P & \longmapsto & (Q \bmod P_1, \dots, Q \bmod P_r) \end{array} \right.$$

Pour $i \in [\![1, r]\!]$, notons $K_i = \mathbf{F}_q[X]/(P_i)$. Comme P_i est irréductible, K_i est un corps (de caractéristique p et de cardinal $p^{\deg(P_i)}$).

Soit $Q \in \mathbf{F}_q[X]/(P)$. Notons $(Q_1, \ldots, Q_r) \in K_1 \times \cdots \times K_r$ l'image de Q par φ.

$$\begin{aligned} Q \in \mathrm{Ker}(S_P - Id) &\Leftrightarrow Q^q - Q = 0 \bmod P \\ &\Leftrightarrow \forall i \in [\![1, r]\!], Q_i^q - Q_i = 0 \bmod P_i \\ &\Leftrightarrow \forall i \in [\![1, r]\!], Q_i^q = Q_i \text{ dans } K_i \\ &\Leftrightarrow \forall i \in [\![1, r]\!], Q_i \in \mathbf{F}_q \\ &\Leftrightarrow (Q_1, \ldots, Q_r) \in \mathbf{F}_q^r \end{aligned}$$

L'avant dernière équivalence vient du fait que, pour tout $i \in [\![1, r]\!]$, $\{x \in K_i | x^q = x\} = \mathbf{F}_q$. En effet, tous les éléments x de $\mathbf{F}_q \subset K_i$ vérifient $x^q = x$ par cyclicité de $\mathbf{F}_q^\times$ et le polynôme $X^q - X$ a moins de q racines dans K_i : comme on en a déjà trouvé exactement q, il n'y en a donc pas d'autres.

On en déduit que $\mathrm{Ker}(S_p - Id) = \varphi^{-1}(\mathbf{F}_q^r)$. Comme φ est un isomorphisme, la dimension de $\mathrm{Ker}(S_p - Id)$ vaut donc r.

(3) On suppose maintenant que $r > 1$. Ceci assure l'existence d'un polynôme $V \in \mathbf{F}_q[X]$ non congru à un polynôme constant modulo P et dont la classe modulo P appartient à $\mathrm{Ker}(S_p - Id)$. Comme la classe de $V \in \mathrm{Ker}(S_P - Id)$, pour tout $i \in [\![1, r]\!]$, $V \bmod P_i = a_i \in \mathbf{F}_q$.

Soit désormais $a \in \mathbf{F}_q$. On note D le pgcd de P et $V - a$: c'est un produit d'éléments de $\{P_i | i \in [\![1, r]\!]\}$ puisqu'il divise P. D'autre part, comme les P_i sont premiers entre eux, D est le produit des P_i tels que P_i divise $V - a$. Or, pour tout $i \in [\![1, r]\!]$, $V - a = a_i - a \bmod P_i$. Donc P_i divise $V - a$ si et seulement si $a_i = a$. On en déduit que $\mathrm{pgcd}(P, V - a) = \prod_{i, a = a_i} P_i$.

Enfin, en partitionnant $[\![1, r]\!]$, on a

$$P = \prod_{i=1}^{r} P_i = \prod_{a \in \mathbf{F}_q} \prod_{i \in [\![1, r]\!], a = a_i} P_i = \prod_{a \in \mathbf{F}_q} \mathrm{pgcd}(\mathrm{P}, \mathrm{V} - \mathrm{a})$$

Tous les facteurs de ce produit divisent P donc sont comme lui sans facteur carré. Ce sont donc des entrées valides pour l'algorithme décrit dans le théorème.

(4) Reste à montrer que l'algorithme décrit ici termine. Pour ce faire, il suffit de montrer que le nombre r de polynômes irréductibles, facteurs de l'entrée de notre algorithme, décroît strictement. C'est le cas car l'un au moins des $\mathrm{pgcd}(P, V - a)$ est un diviseur strict de P.

En effet, V n'est pas constant modulo P donc il existe $i \neq j$ tel que $a_i \neq a_j$ (sinon, tous les a_i sont égaux à $a \in \mathbf{F}_q$ et $V - a$ est divisible par tous les P_i donc par leur produit puisqu'ils ont premiers entre eux. Alors $V = a \bmod P$ ce qui contredit que V est non constant modulo P). On a donc $P_i | \mathrm{pgcd}(P, V - a_i)$ donc $\deg(\mathrm{pgcd}(P, V - a_i)) > 0$ et $P_j \nmid \mathrm{pgcd}(P, V - a_i)$ donc $\deg(\mathrm{pgcd}(P, V - a_i)) < \deg(P)$.

Algorithme de factorisation :
Soit $P \in \mathbf{F}_q[X]$.

- Si $P' = 0$ alors il existe $R \in \mathbf{F}_q[X]$ tel que $P = R^p$. Les coefficients de R ce calculent comme racines p-èmes des coefficients de P. Ré-appliquer l'algorithme à R.
- Si $P' \neq 0$ et $D = \text{pgcd}(P, P') \neq 1$ alors D est un diviseur strict de P et on ré-applique l'algorithme à D et P/D.
- Si $P' \neq 0$ et $D = \text{pgcd}(P, P') = 1$, alors P est sans facteurs carrés donc on peut lui appliquer l'algorithme de Berlekamp décrit ci-dessus et on s'empresse de le faire.

Questions

③ Ch. des pol. irr de deg 4 sur $\mathbb{F}_q$

④ $P = P_1^{m_1} P_2^{m_2}$

$P' = m_1 P_1' P_1^{m_1 - 1} P_2^{m_2} + m_2 P_2' P_2^{m_2 - 1} P_1^{m_1}$

② $X^4 + 1 \in \mathbb{F}_p[X]$, $\mathbb{F}_{p^2}$

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Si $p \equiv 1 \bmod 4$ -1 carré

$X^4 + 1 = X^4 - (-1) = X^4 - a^2 = (X^2 + a)(X^2 - a)$

$(X^4 + 1) = (X+1)^4$ sur $\mathbb{F}_2[X]$

THÉORÈME DE CHEVALLEY-WARNING

VLADISLAV TEMPEZ

Référence : Jean Pierre Serre, Cours d'arithmétique page 12.
Théorème: Chevalley-Warning
Soit $\mathbf{K}$ un corps fini de la forme $\mathbf{F}_q$ où $q = p^d$ est une puissance d'un nombre premier p.

Soit $(f_i)_{1\leq i\leq r}$ une famille de polynômes de $\mathbf{K}[X_i]_{1\leq i\leq n}$ tels que $\sum\limits_{i=1}^{r} \deg(f_i) < n$
On note $Z = \{x \in (\mathbf{F}_q)^n | \ \forall i \in [\![1, r]\!], \ f_i(x) = 0\}$ et on a $\mathrm{Card}(Z) \equiv 0[p]$.

Démonstration:

On montre tout d'abord le lemme suivant.

Lemme:

Soit $\mathbf{K}$ un corps fini de la forme $\mathbf{F}_q$ où $q = p^d$ est une puissance d'un nombre premier p et $u \in \mathbf{N}$.

On note $S(X^u) = \sum\limits_{x\in\mathbf{K}} x^u$ et on a

$$S(X^u) = \begin{cases} -1 \text{ si } u \geq 1 \text{ et } q-1|u \\ 0 \text{ sinon} \end{cases}$$

On utilise la convention $0^0 = 1$.

Démonstration:

Si $u = 0$, $S(X^u) = \sum\limits_{x\in\mathbf{K}} 1 = q \equiv 0[p]$.
Si $u \geq 1$ et $q-1|u$.
$\mathbf{K}^\times$ est cyclique d'ordre $q-1$ donc $\forall x \in \mathbf{K}^\times, \ x^u = 1$.
On a alors

$$S(X^u) = \sum_{x\in\mathbf{K}^\times} 1 = q - 1 \equiv -1[p]$$

Si $u \geq 1$ et $q - 1 \nmid u$ on a toujours $\mathbf{K}^\times$ cyclique d'ordre $q-1$ donc il existe y d'ordre $q-1$, donc $y^u \neq 1$.

On a aussi $\mathbf{K} = y\mathbf{K}$ car y inversible. Ainsi

$$S(X^u) = \sum_{x\in\mathbf{K}} x^u = \sum_{x\in\mathbf{K}} y^u x^u = y^u S(X^u)$$

Donc on a $(1-y^u)S(X^u) = 0$ avec $y \neq 1$ dans $\mathbf{K}$ qui est intègre, donc $S(X^u) = 0$.
Le lemme est donc démontré.

On pose $P = \prod_{i=1}^{r}(1 - f_i^{q-1})$ un élément de $\mathbf{K}[X_i]_{1\leq i\leq n}$. Montrons que P vaut 1 sur Z et 0 partout ailleurs.

Si $x \in Z$, $P(x) = \prod_{i=1}^{r}(1 - f_i^{q-1}(x)) = 1$ car $\forall i \in [\![1, r]\!]$, $f_i(x) = 0$.

Si $x \notin Z$, il existe $1 \leq i \leq r$, $f_i(x) \neq 0$. Or $\mathbf{K}^\times$ cyclique d'ordre $q-1$ donc $f_i(x)^{q-1} = 1$ et ainsi $P(x) = 0$.

On va étendre S sur $\mathbf{K}[X_i]_{1\leq i\leq n}$ de la manière suivante : $S(f) = \sum_{x\in\mathbf{K}^n} f(x)$.

On a en particulier $\mathrm{Card}(Z) \equiv S(P)[p]$.

Soit $X^u = \prod_{i=1}^{n} X_i^{u_i}$ un monôme de P. On a

$$S(X^u) = \sum_{x\in\mathbf{K}^n}\prod_{i=1}^{n} x_i^{u_i} = \prod_{i=1}^{n}\sum_{x_i\in\mathbf{K}} x_i^{u_i} = \prod_{i=1}^{n} S(X_i^{u_i})$$

Or, $\deg(\mathrm{P}) \leq \sum_{i=1}^{r}\deg(f_i)(q-1) < n(q-1)$ donc pour tout monôme X^u de P,

$$\sum_{i=1}^{n} u_i < n(q-1)$$

donc il existe i tel que $u_i < q-1$ et ainsi, par le lemme $S(X_i^{u_i}) \equiv 0[p]$ donc $S(P) \equiv 0[p]$.

On peut donc conclure que $\mathrm{Card}(Z) \equiv 0[p]$.

Corrolaire:

Pour une famille (f_i) de polynômes sans facteurs constants, 0 est une racine commune donc $\mathrm{Card}(Z) \geq p$. En particulier pour une forme quadratique de trois variables il existe au moins un 0 non trivial.