121 Nombres premiers. Applications.

I- ARITHMETIQUE DANS $\mathbb{Z}$

1) DIVISIBILITE PAIRS $\mathbb{Z}$

Def 1: On dit que $n \in \mathbb{N}$ est un nombre premier si $n \neq 1$ et n n'admet pas d'autres diviseurs dans $\mathbb{N}$ que 1 et n.

Not 2: On note $\mathcal{P}$ l'ensemble des nombres premiers.

Prop 3: Tout entier $n \geq 2$ possède un diviseur premier.

Prop 4: Lemme d'Euclide

Si p est premier, alors $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$

Prop 5: Théorème fondamental de l'arithmétique

Tout nombre entier différent de 0 ou 1 se décompose de manière unique en produit de nombres premiers

Cor 6: $\mathcal{P}$ est infini.

Prop 6: Soit $a, b \in \mathbb{Z}$. $(a,b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Cor 7: Soit $n \in \mathbb{N}$. $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow n$ est premier.

2) FONCTIONS ARITHMETIQUES.

Def 8: On appelle fonction arithmétique toute fonction $f : \mathbb{N}^* \to \mathbb{C}$. On note $\mathcal{A}$ leur ensemble.

Ex 9:
- $d(n)$: nombre de diviseurs de n.
- $\varphi(n)$: nombre d'entiers m tels que $1 \leq m \leq n$ et $n \wedge m = 1$ (Indicatrice d'Euler)
- $\mu(n) = \begin{cases} 0 \text{ si } n \text{ est divisible par le carré d'un nombre premier} \\ (-1)^k \text{ si } n \text{ se décompose en un nombre impair } k \text{ de facteurs premiers distincts} \\ 1 \text{ sinon.} \end{cases}$ (Fonction de Möbius)
- $\mathbb{1}(n) = 1 \quad \forall n \in \mathbb{N}^*$

Def 10: Une fonction arithmétique est dite multiplicative si : $\forall (m,n) \in (\mathbb{N}^*)^2, ((m,n) = 1 \Rightarrow f(mn) = f(m)f(n)]$ et $f \neq 1$

On note $\mathcal{M}$ leur ensemble.

Cons 11: Si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ avec les p_i distincts, alors : $f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_i})$

Ex 12: $\varphi(n) = n \prod_{p \in \mathcal{P} \atop p \mid n} \left(1 - \frac{1}{p}\right)$ est multiplicative.

Def 13: $f \in \mathcal{A}$ est dit complètement multiplicative si : $\forall (m,n) \in (\mathbb{N}^*)^2, f(mn) = f(m)f(n)$ et $f(1) = 1$.

Ex 14: Soit $p \in \mathcal{P} \setminus \{2\}$. La fonction définie par : $\forall n \in \mathbb{N}^*$, $\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \bmod p$ est complètement multiplicative. On l'appelle le symbole de Legendre.

Prop 15: $(\mathcal{A}, +, \times, *)$ est une algèbre unitaire commutative, où $+, \times$ sont les lois usuelles, et $\forall f, g \in \mathcal{A}$, $\forall n \in \mathbb{N}^*$, $f * g(n) = \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right)$. Son élément neutre est : $e(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon} \end{cases}$

Prop 16: $(\mathcal{M}, *)$ est un sous-groupe de l'ensemble des inversibles de $\mathcal{A}$.

Prop 17: $\mu * \mathbb{1} = e$

Cor 18: Formule d'inversion de Möbius : Soit $f, g \in \mathcal{A}$.

Alors $\left[\forall n \in \mathbb{N}^*, g(n) = \sum_{d \mid n} f(d)\right] \Leftrightarrow \left(\forall n \in \mathbb{N}^*, f(n) = \sum_{d \mid n} \mu(d) g\left(\frac{n}{d}\right)\right)$

i.e. $g = f * \mathbb{1} \Leftrightarrow f = \mu * g$.

Ex 19: $n = \sum_{d \mid n} \varphi(d) \Rightarrow \varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}$

Def 20: Une série de Dirichlet est une série de fonctions de la variable complexe s, de la forme $\sum_{n \geq 1} \frac{f(n)}{n^s}$ où $f \in \mathcal{A}$.

Prop 21: Si $f, g \in \mathcal{A}$, alors $\left(\sum_{n=1}^{+\infty} \frac{f(n)}{n^s}\right)\left(\sum_{n=1}^{+\infty} \frac{g(n)}{n^s}\right) = \left(\sum_{n=1}^{+\infty} \frac{f*g(n)}{n^s}\right)$

3) REPARTITION DES NOMBRES PREMIERS

Prop 22: Il existe une infinité de nombres premiers de la forme $4n+3$.

Prop 23 : Théorème de Dirichlet (ADMIS)
Si $(a,b)=1$, alors il existe une infinité de nombres premiers de la forme $an+b$.

Prop 24 : La série $\sum_{p\in\mathcal{P}} \frac{1}{p}$ diverge

Th. 25 : Théorème des nombres premiers (ADMD)
On pose $\forall x\in\mathbb{R}_+$, $\pi(x)=\mathrm{Card}(\mathcal{P}\cap[0,x])$. On a $\pi(x)\underset{+\infty}{\sim}\frac{x}{\ln x}$

I FCORPS FINIS

1) Construction

[PER]

Déf 26 : Soit K un corps fini. Le noyau de $\varphi : \begin{cases}\mathbb{Z}\to K\\ n\mapsto n.1_K\end{cases}$ est de la forme $p\mathbb{Z}$, avec $p\in\mathcal{P}$. On note $p=\mathrm{Car}(K)$, et on l'appelle caractéristique de K.

Rq 27 : Si $\mathrm{car}(K)=p$, le sous-corps premier de K est $\mathbb{Z}/p\mathbb{Z}$. K a alors une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel, et on dispose de $n\in\mathbb{N}^*$ tel que $|K|=p^n$.

Déf 28 : L'application $F : \begin{cases}K\to K\\ x\mapsto x^p\end{cases}$ est un isomorphisme de corps appelé morphisme de Frobenius.

Prop 29 : Petit théorème de Fermat
Soit $p\in\mathcal{P}$, $\forall a\in\mathbb{Z}$, $a^p\equiv a \bmod p$

Prop 30 : Soit $p\in\mathcal{P}$, $n\in\mathbb{N}^*$. On pose $q=p^n$.
i) Il existe un corps à q éléments, c'est le corps de décomposition du polynôme X^q-X sur $\mathbb{F}_p$.
ii) Ce corps est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Prop 31 : Théorème de Wilson. Soit $p\in\mathbb{N}\setminus\{0,1\}$.
Alors p premier $\iff (p-1)!\equiv -1 \bmod p$

Prop 32 : Soit $p\in\mathcal{P}$, $n\in\mathbb{N}$ et $q=p^n$.
i) K sous-corps de $\mathbb{F}_q \Rightarrow \exists d\mid n$ tel que $|K|=p^d$
ii) $\forall d\mid n$, $\mathbb{F}_q$ a un sous-corps de cardinal p^d (c'est le corps de décomposition de $X^{p^d}-X$ sur $\mathbb{F}_p$ dans $\mathbb{F}_q$)

Prop 33 : $\mathbb{F}_q^*$ est cyclique.

2) Polynômes irréductibles

[GOZ]

Prop 34 : Critère d'Eisenstein. Soit $P=\sum_{i=0}^{n} a_i X^i \in\mathbb{Z}[X]$.
S'il existe $p\in\mathcal{P}$ tel que $p\nmid a_n$, $\forall i\in\{0,\dots,n-1\}$, $p\mid a_i$ et $p^2\nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$.

Prop 35 : Soit $P=\sum_{i=0}^{n} a_i X^i\in\mathbb{Z}[X]$, $\deg P\geq 1$ et $p\in\mathcal{P}$ tel que $p\nmid a_n$. Si $P\bmod p$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

Prop 36 : Soit $p\in\mathcal{P}$ et $n\in\mathbb{N}^*$. Posons $q=p^n$. Alors pour tout polynôme irréductible sur $\mathbb{F}_p$ de degré n, $\mathbb{F}_q=\frac{\mathbb{F}_p[X]}{(\pi)}$

Cor 37 : Un polynôme irréductible sur $\mathbb{F}_p$ de degré n est scindé sur $\mathbb{F}_{p^n}$. Son corps de rupture est donc aussi son corps de décomposition.

Th. 38 : Soit $p\in\mathcal{P}$, $n\in\mathbb{N}^*$. On note $q=p^n$, et pour $j\in\mathbb{N}^*$ $\mathrm{Irr}(p,j)$ l'ensemble des polynômes irréductibles sur $\mathbb{F}_p$ de degré j. On a : $X^q-X=\prod_{d\mid n}\prod_{Q\in\mathrm{Irr}(p,d)} Q$

Th 39 : On a $p^n=\sum_{d\mid n} d\,|\mathrm{Irr}(p,d)|$ donc $|\mathrm{Irr}(p,n)|=\frac{1}{n}\left(\sum_{d\mid n}\mu(d)\,p^{\frac{n}{d}}\right)\underset{+\infty}{\sim}\frac{p^n}{n}$

Ex 40 : $\mathbb{F}_4=\mathbb{F}_2[X]/(X^2+X+1)$, $\mathbb{F}_8=\mathbb{F}_2[X]/(X^3+X+1)$
$=\mathbb{F}_2[X]/(X^3+X^2+1)$

3) Carrés dans $\mathbb{F}_q$ ($q=p^n$)

[CAL]

Th 41 : Si $p=2$, tout élément de $\mathbb{F}_q$ est un carré.
Si $p\neq 2$, $(\mathbb{F}_q^*)^2$ forme un sous-groupe d'ordre 2 de $\mathbb{F}_q^*$, c'est le noyau du morphisme $\begin{cases}\mathbb{F}_q^*\to\{-1,1\}\\ x\mapsto x^{\frac{q-1}{2}}\end{cases}$

Prop 42 : $\forall p\in\mathcal{P}$ impair, $\forall a\in\mathbb{F}_p$,
$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{si } a\in(\mathbb{F}_p^*)^2\\ -1 & \text{si } a\notin(\mathbb{F}_p^*)^2\\ 0 & \text{sinon}\end{cases}$$

Cor 43 : $\forall p\in\mathcal{P}$ impair, $\forall a\in\mathbb{F}_p$, $|\{x\in\mathbb{F}_p,\ ax^2=1\}|=1+\left(\frac{a}{p}\right)$

Ex 44 : Pour $p\in\mathcal{P}$ impair,
$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & \text{si } p\equiv 1 \bmod 4\\ -1 & \text{si } p\equiv 3 \bmod 4\end{cases}$$

DEV n°1 [SERE]

Th 45 : Classification des formes quadratiques sur $\mathbb{F}_q$ à $\mathrm{Cor}(\mathbb{F}_q)^{*2}$.
Soit E un $\mathbb{F}_q$-ev de dimension n. Soit $\alpha \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$.
Alors il y a deux classes d'équivalence de formes quadratiques sur E, de matrices :
$Q_1 = I_n$ et $Q_2 = \mathrm{diag}(1, \dots, 1, \alpha)$

Th 46 : Loi de réciprocité quadratique. Soit $p, q \in \mathcal{P}$ impairs, avec $p \neq q$. Alors $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$.

III - CORPS p-ADIQUES

1) CONSTRUCTION

Def 47 : Soit $n \geq 1$. On note $A_n = \mathbb{Z}/p^n\mathbb{Z}$ et $\varphi_n : A_n \to A_{n-1}$ le morphisme canonique. On appelle anneau des entiers p-adiques $\mathbb{Z}_p$, le sous-anneau de $\prod_{n\geq 1} A_n$ tel que $x \in \mathbb{Z}_p$ ssi $\forall n \geq 2$ $\varphi_n(x_n) = x_{n-1}$.

Prop 48 : Soit $\zeta_n : \mathbb{Z}_p \to A_n$ l'application coordonnées. La suite $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\zeta_n} A_n \to 0$ est exacte.
(i.e. on peut identifier A_n et $\mathbb{Z}_p/p^n\mathbb{Z}_p$)

Prop 49 : L'ensemble des inversibles de $\mathbb{Z}_p$ est $U = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

Prop 50 : Tout $x \in \mathbb{Z}_p$ s'écrit de manière unique $x = p^k u$ avec $u \in U$ et $k \in \mathbb{N}$.
On note $k = v_p(x)$; on l'appelle valuation p-adique de x.

Def 51 : On note $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$. On l'appelle corps des nombres p-adiques.
On étend v_p à $\mathbb{Q}_p$ en posant $\forall x \in \mathbb{Z}_p, \forall y \in U$, $v_p\left(\frac{x}{y}\right) := v_p(x) - v_p(y)$

2) TOPOLOGIE

Def/Prop 52 : Par convention, on pose $v_p(0) = +\infty$. On munit $\mathbb{Q}_p$ de la norme : $|x|_p = p^{-v_p(x)}$.

Rq 53 :
- $\mathbb{Q}_p$ est le complété de $\mathbb{Q}$ pour $|.|_p$.
- la distance associée à $|.|_p$ est dite ultramétrique, i.e. $d_p(x,z) \leq \max(d_p(x,y), d_p(y,z))$, $\forall z \in \mathbb{Q}_p$.

Prop 54 : $\mathbb{Z}_p$ est compact, et $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$

Prop 55 : $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$.

3) EQUATION p-ADIQUES

Th 56 : Soit $f \in \mathbb{Z}_p[X_1, \dots, X_n]$, $x = (x_i) \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ et $j \in \{1, \dots, m\}$. On suppose $0 \leq 2k < n$ et que :
$f(x) \equiv 0 \bmod p^n$ et $v_p\left(\frac{\partial f}{\partial x_j}(x)\right) = k$
Il existe alors un zéro y de f dans $\mathbb{Z}_p^m$ qui est congru à x modulo p^{n-k}.

Cor 57 : Supposons $p \neq 2$ et soit q une forme quadratique sur $\mathbb{Z}_p$ telle que $\mathrm{Disc}(q) \in U$. Soit $a \in \mathbb{Z}_p$.
Si $x \in \mathbb{Z}_p^n$ vérifie : $\exists i, x_i \in U$ et $f(x) \equiv a \bmod p$, alors il existe $\tilde{x} \in \mathbb{Z}_p^n$ tel que $f(\tilde{x}) = a$.

DEV n°2 [CON

IV - RECHERCHE ET UTILISATION DES NOMBRES PREMIERS

1) CRYPTAGE chiffrement

Th 58 : Soit $p, q \in \mathcal{P}$, $p \neq q$. Soit $c, d \in \mathbb{N}$.
Si $cd \equiv 1 \bmod (p-1)(q-1)$, alors $\forall x \in \mathbb{N}$, $x^{cd} \equiv x \bmod pq$

CRYPTAGE RSA : Soit $p, q \in \mathcal{P}$, $p \neq q$. On pose $n = pq$.
Un message $x \in \mathbb{Z}/n\mathbb{Z}$, chiffré en $C(x) = x^e$ est adressé à une personne qui est la seule à détenir la clé secrète $D(y) = y^d$.
Cette personne applique D au message pour retrouver x.

2) TESTS DE PRIMALITE

Ex 59 : Crible d'Eratosthène

Def 60 : Un nombre de Fermat est un nombre de la forme $F_k = 2^{2^k} + 1$

Ex 61 : Pour $k \in \{1, 2, 3, 4\}$, F_k est premier. Mais F_5 n'est pas premier.
(plus généralement, F_k n'est pas premier pour $5 \leq k \in 2\mathbb{N}$)

Def 62 : Un nombre de Mersenne est de la forme $M_r = 2^r - 1$ avec $r \in \mathcal{P}$.

Rq 63 : Les nombres de Mersenne ont fourni les plus grands nombres premiers connus.

Prop 64 : Test de Lucas-Lehmer. Soit $u = 2 + \sqrt{3}$ et $v = 2 - \sqrt{3}$. Pour $n \in \mathbb{N}$, posons $S_n = u^{2^n} + v^{2^n}$. Alors : (i) (S_n) est une suite d'entiers, et $S_{n+1} = S_n^2 - 2$
(ii) Si $M_p \mid S_{p-2}$, alors M_p est premier.

Haut minerai

Références :

[MER] Fondamentaux d'algèbre et d'arithmétique, Dany-Jack Mercier.

[PAR] Exercices in Number Theory, D.P. Parent.

[PER] Cours d'algèbre, Daniel Perrin.

[GOZ] Théorie de Galois, I. Gozard.

[CAL] Histoires Hédonistes de Groupes de Géométrie, Caldero - Germoni.

[SER] Cours d'arithmétique, Jean-Pierre Serre.

[COM] Algèbre et géométrie, François Combes.

Loi de réciprocité quadratique

Références : Histoires hédonistes de groupes et de géométrie, Caldero-Germoni.

Soit $p > 2$ premier.

Définition 0.1

Le symbole de Legendre est l'application:

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \longrightarrow \{-1, 1\}$$
$$a \longmapsto a^{\frac{p-1}{2}}$$

On remarque que, pour tout $a \in \mathbb{F}_p^*$, $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 1 + (\frac{a}{p})$.

Théoreme 0.1

Soit $p \neq q$ deux nombres premiers impairs. Alors,

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

Démonstration: On calcule le cardinal de $X = \{(x_1, ..., x_p) \in (\mathbb{F}_q)^p, \sum_{i=1}^p x_i^2 = 1\}$ de 2 façons.

(1) On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X via $k.(x_1, .., x_p) = (x_{k+1}, .., x_{k+p})$, avec des indices modulo p.
Par la formule des classes, on sait que $|X| = |X^{\mathbb{Z}/p\mathbb{Z}}|[p]$.
Or

$$\begin{aligned}(x_i) \in X^{\mathbb{Z}/p\mathbb{Z}} &\Leftrightarrow \forall k \in \mathbb{Z}/p\mathbb{Z} \qquad k.(x_i) = (x_i) \in X \\ &\Leftrightarrow \exists x \in \mathbb{F}_q \quad \forall 1 \leqslant i \leqslant p \qquad x_i = x \qquad \text{et} \qquad px^2 = 1\end{aligned}$$

Donc $|X| = 1 + (\frac{p}{q})[p]$

(2) On rappelle que deux formes quadratiques définies sur $\mathbb{F}_q$ sont équivalentes ssi elles sont de même rang et de même discriminant sur $\mathbb{F}_q$.
On pose $d = \frac{p-1}{2}$ et

$$f(X_1, .., X_n) = \sum_{i=1}^{p} X_i^2$$

$$g(Y_1, ..., Y_d, Z_1, ..., Z_d, T) = 2\sum_{i=1}^{d} Y_i Z_i + (-1)^d T^2$$

On note que $f \sim g$ donc $X = \{x \in (\mathbb{F}_q)^p, f(x) = 1\}$ s'identifie à $X' = \{x \in (\mathbb{F}_q)^p, g(x) = 1\}$ par un changement de variables linéaire.
Soit $x = (y_1, ..., y_d, z_1, ..., z_d, t) \in X'$.
Si pour tout $0 \leqslant i \leqslant d$ $y_i = 0$, on a $q^d\Big(1 + \big((-1)^d\big)^{\frac{q-1}{2}}\Big)$ possibilités. Sinon, à y_1,..., y_d et t sont fixés, il reste à choisir z_1,..., z_d dans un hyperplan affine de $(\mathbb{F}_q)^d$, ce qui fait $(q^d - 1)qq^{d-1}$ possibilités.

D'où $|X| = q^d\Big(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big)$. Donc dans $\mathbb{F}_p$,

$$\begin{aligned} |X| &= (\frac{q}{p})\Big((\frac{q}{p}) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big)[p] \\ (\frac{q}{p})\big(1 + (\frac{p}{q})\big) &= (\frac{q}{p})^2\Big((\frac{q}{p}) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big)[p] \\ (\frac{p}{q})(\frac{q}{p}) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}[p] \end{aligned}$$

Racines d'un polynôme à coefficients dans $\mathbb{Z}_p$

Références : Cours d'arithmétique, Serre, p.28-30.

Soit p premier.

Théoreme 0.1

Soit $m \in \mathbb{N}^*$ et $f \in \mathbb{Z}_p[X_1, ..., X_m]$, $x = (x_i) \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ et $j \in \{1, .., m\}$. On suppose que $0 \leqslant 2k < n$ et que

$$f(x) = 0[p^n] \quad et \quad |\frac{\partial f}{\partial X_j}(x)|_p = p^{-k}.$$

Alors il existe $y \in (\mathbb{Z}_p)^m$ tel que

$$f(y) = 0 \qquad et \qquad y = x[p^{(n-k)}]$$

La démonstration utilise le lemme d'Hensel qui est un analogue p-adique de la méthode de Newton.

Lemme 0.1

Soit $f \in \mathbb{Z}_p[X]$, $x \in \mathbb{Z}_p$ et $0 \leqslant 2k < n$. On suppose

$$f(x) = 0[p^n] \quad et \quad |f'(x)|_p = p^{-k}.$$

Alors il existe $y \in \mathbb{Z}_p$ tel que

$$f(y) = 0[p^{n+1}], \qquad |f'(y)|_p = p^{-k}, \qquad y = x[p^{n-k}]$$

Démonstration: (du lemme) Pour satisfaire la dernière condition, on pose $y = x + p^{n-k}z$ avec $z \in \mathbb{Z}_p$. Par la formule de Taylor-Young, il existe $a \in \mathbb{Z}_p$

$$f(y) = f(x) + f'(x)p^{n-k}z + p^{2(n-k)}a$$

On écrit $f(x) = p^n b$, $b \in \mathbb{Z}_p$, et $f'(x) = p^k c$, $c \in \mathbb{Z}_p^*$. On rappelle que $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash p\mathbb{Z}_p$. On a $b = bc^{-1}c[p]$. On choisit $z = -bc^{-1}$. Alors,

$$f(y) = p^n(b + zc) + p^{2(n-k)}a$$

Comme $2n - 2k > n$, on obtient $f(y) = 0[p^{n+1}]$. De plus, par Taylor-Young à l'ordre 1 sur f', on trouve

$$f'(y) = p^k c[p^{n-k}]$$

Comme $n - k > k$, on a $|f'(y)|_p = p^{-k}$.

Démonstration: Soit $g \in \mathbb{Z}_p[X_j]$ le polynôme obtenu en évaluant f en $(x_i)_{i \neq j}$. Supposons que l'on peut construire une solution y_j pour g. En posant $y_i = x_i$ pour tout $i \neq j$, on aura démontré le théorème.

On a donc réduit le problème à $f \in \mathbb{Z}_p[X]$.

On pose $x^{(0)} = x$. On construit une suite $(x^{(q)}) \in \mathbb{Z}_p^{\mathbb{N}}$ en appliquant le lemme pour $x^{(q)}$ à l'étape $q + 1$. Il existe $x^{(q+1)} \in \mathbb{Z}_p$ tel que

$$f(x^{(q+1)}) = 0[p^{n+q}], \qquad |f'(x^{(q+1)})|_p = p^{-k}, \qquad x^{(q+1)} = x^{(q)}[p^{n+q-k}]$$

En particulier $|x^{(q)} - x^{(q-1)}|_p \leqslant p^{-(n+q-k)}$. Comme la distance p-adique est ultramétrique, on a

$$\forall r > s \quad |x^{(r)} - x^{(s)}|_p \leqslant p^{-(n+s-k)}$$

Donc $(x^{(q)})$ est de Cauchy dans $\mathbb{Z}_p$ complet. Ainsi, il existe $y \in \mathbb{Z}_p$ limite de $(x^{(q)})$ pour la distance p-adique.

Alors $f(y) = 0$ et $y = x[p^{n-k}]$.

Propriété 0.1

On suppose $p \neq 2$. Soit f une forme bilinéaire symétrique de coefficients $(a_{ij})_{i,j \leqslant m} \in (\mathbb{Z}_p)^{m^2}$ tels que $\det(a_{ij}) \in \mathbb{Z}_p^*$. Soit $a \in \mathbb{Z}_p$ et $x = (x_i) \in (\mathbb{Z}_p)^m$ tel que

$$\exists j \in 1, .., m \quad x_j \in \mathbb{Z}_p^* \qquad et \qquad f(x) = a[p]$$

Alors il existe une solution exacte issue de x.

Démonstration: On souhaite appliquer le théorème pour $n = 1$ et $k = 0$. Supposons que pour tout l, $\frac{\partial f}{\partial X_l} = 0[p]$. Or,

$$\forall l \in 1, .., m \quad \frac{\partial f}{\partial X_l}(x) = 2\sum_i a_{il} x_i$$

Alors, en notant $A = (a_{ij})$, on a $2Ax = 0[p]$. Mais par hypothèse $x_j \neq 0[p]$. On a contredit $\det(a_{ij}) \in \mathbb{Z}_p^*$.