120 Anneau $\mathbb{Z}/n\mathbb{Z}$. Applications

déf 1: On dit que x est congru à y modulo n, noté $x \equiv y\ [n]$ si $x-y \in n\mathbb{Z}$.

I Structures de $\mathbb{Z}/n\mathbb{Z}$

1) Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

[GOU] p18 **Prop 2**: Tous les sous groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.

Rq 3: Ils sont tous commutatifs donc distingués.

Prop 4: $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

[RB] p13 **Prop 5**: · $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique
· $\bar{a}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +) \Leftrightarrow a \wedge n = 1$

[RB] p11 **Prop 6**: · Tout groupe monogène est isomorphe soit à $(\mathbb{Z}, +)$ soit à $(\mathbb{Z}/n\mathbb{Z}, +)$.
· Tout groupe cyclique est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

[RB] p11 **Prop 7**: Tout sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.

Appli 8: Tout sous-groupe d'un groupe cyclique est cyclique.

[PER] p13 **Cor 9**: $\mathbb{Z}/p\mathbb{Z}$ est simple $\Leftrightarrow p$ est premier.

2) Anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

[GOU] p19 **Prop 10**: $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Prop 11: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif

p64 **Prop 12**: $\mathbb{Z}/p\mathbb{Z}$ est un corps $\Leftrightarrow p$ est premier
$\Leftrightarrow \mathbb{Z}/p\mathbb{Z}$ est intègre

[RB] p16 **Thm 13**: (Chinois) Soient $m_1, m_2 \in \mathbb{N}^*$ tq $m_1 \wedge m_2 = 1$
Alors
$$\psi : \begin{array}{ccc} \mathbb{Z}/m_1m_2\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \\ \bar{k} & \longmapsto & (\bar{k}_1, \bar{k}_2) \end{array}$$
est un isomorphisme d'anneaux.

Cor 14: $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ [PER] p25

Cor 15: Soit $m = m_1 \dots m_s \in \mathbb{Z}$ avec $m_i > 1$ et $\forall i \neq j\ \ m_i \wedge m_j = 1$ [RB] p17
Alors $\forall a, b \in \mathbb{Z}$ $\quad a \equiv b\ [m] \Leftrightarrow \forall i\ a \equiv b\ [m_i]$

Ex 16: Résoudre $\begin{cases} x \equiv 3 \bmod 13 \\ x \equiv 7 \bmod 19 \end{cases}$

II Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$

1) Fonction indicatrice d'Euler

Prop 17: $a \wedge n = 1 \Leftrightarrow \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ [PER] p24

Déf 18: (fonction indicatrice d'Euler)
$\varphi(n) = \mathrm{card}\,(\mathbb{Z}/n\mathbb{Z})^*$

Ex 19: Si p premier et $k \in \mathbb{Z}$ $\quad \varphi(p) = p-1$ et $\varphi(p^k) = (p-1)p^{k-1}$.

Prop 20: Soient m_1, m_2 tq $m_1 \wedge m_2 = 1$ [RB] p18
$(\mathbb{Z}/m_1m_2\mathbb{Z})^* \simeq (\mathbb{Z}/m_1\mathbb{Z})^* \times (\mathbb{Z}/m_2\mathbb{Z})^*$

Cor 21: Si $m_1 \wedge m_2$ $\quad \varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$

Prop 22: Soit G un groupe cyclique d'ordre n. [RB] p14
Alors pour tout $d>0$ tel que $d \mid n$, il y a, dans G, $\varphi(d)$ éléments d'ordre d.

Cor 23: $\sum_{d \mid n} \varphi(d) = n$

Thm 24: (d'Euler) Si $a \wedge n = 1$ [RB] p15
alors $a^{\varphi(n)} \equiv 1\ [n]$.

Thm 25: (de Fermat) Soient p premier et a tel que $p \nmid a$ alors $a^{p-1} \equiv 1\ [p]$. $\quad$ ex: $10^{10^n} \equiv 4\ [7]$ [XENS] p111

Déf 26: On dit que n est un nombre de Carmichaël si n n'est pas premier et que $\forall a \in \mathbb{Z}$ tq $a \wedge n = 1 \Rightarrow a^{n-1} \equiv 1\ [n]$

Ex 27 : 561 est le plus petit nombre de Carmichaël.

2) Automorphismes de $(\mathbb{Z}/_{n\mathbb{Z}})$

[PER] p24-25 -26 Prop 28 : $Aut(\mathbb{Z}/_{n\mathbb{Z}}) \simeq (\mathbb{Z}/_{n\mathbb{Z}})^*$

Prop 29 : $(\mathbb{Z}/_{p\mathbb{Z}})^* \simeq (\mathbb{Z}/_{(p-1)\mathbb{Z}})$ $\forall p$ premier

Prop 30 : $(\mathbb{Z}/_{n\mathbb{Z}})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/_{p_i^{\alpha_i}\mathbb{Z}})^*$

Prop 31 : Soient p premier ≥ 3 et $\alpha \geq 2$

$$(\mathbb{Z}/_{p^\alpha\mathbb{Z}})^* \simeq \mathbb{Z}/_{\varphi(p^\alpha)\mathbb{Z}} \simeq \mathbb{Z}/_{(p-1)p^{\alpha-1}\mathbb{Z}}$$

Prop 32 : · $(\mathbb{Z}/_{4\mathbb{Z}})^* \simeq \mathbb{Z}/_{2\mathbb{Z}}$

· $\forall \alpha \geq 3$ $(\mathbb{Z}/_{2^\alpha\mathbb{Z}})^* \simeq \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2^{\alpha-2}\mathbb{Z}}$

III Groupes, corps et $\mathbb{Z}/_{n\mathbb{Z}}$

[COM] p66 Prop 33 : Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe $q_1, \dots, q_k$ entiers tels que $q_1 \geq 2$ et $q_1 | q_2 | \dots | q_k$ uniques et tels que

$$G \simeq \mathbb{Z}/_{q_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{q_k\mathbb{Z}}.$$

[PER] p72 Prop 34 : Soit K un corps fini de caractéristique p. Le sous corps premier de K est isomorphe à $\mathbb{Z}/_{p\mathbb{Z}}$. On le note aussi $\mathbb{F}_p$.

(*) IV Théorie des nombres

1) Polynômes dans $\mathbb{Z}[X]$

[SOU] p58 Thm 35 : (Critère d'Eisenstein)

Soit $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$

S'il existe p premier tel que :

i) $p | a_k$ $\forall 0 \leq k \leq n-1$

ii) $p \nmid a_n$

iii) $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$.

Si de plus $pgcd(a_i) = 1$ alors P est aussi irréductible dans $\mathbb{Z}[X]$.

Appli 36 : Soit p premier. Alors le polynôme $X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Z}[X]$. [PER] p77

Thm 37 : (Réduction) Soient $P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Z}[X]$ et $\overline{P}$ sa réduction dans $\mathbb{Z}/_{p\mathbb{Z}}$ avec p premier. Si $\overline{a_n} \neq 0$ (ie $p \nmid a_n$). Alors si $\overline{P}$ est irréductible dans $\mathbb{Z}/_{p\mathbb{Z}}[X]$, le polynôme P est irréductible dans $\mathbb{Q}[X]$.

Appli 38 : $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$ (réduction modulo 2).

2) Résidus quadratiques

Déf 39 : (Symbole de Legendre)

Soient p premier impair et $x \in \mathbb{Z}$

On pose $\left(\frac{x}{p}\right) = \begin{cases} 0 \text{ si } p | x \\ 1 \text{ si } x \text{ est un carré dans } \mathbb{Z}/_{p\mathbb{Z}} \\ -1 \text{ sinon} \end{cases}$ [DUV] p64

Prop 40 : Soit p premier impair et $x \in \mathbb{Z}$. p65

Alors $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod p$.

Cor 41 : Soit p premier impair. [PER

Alors (-1) est un carré dans $\mathbb{Z}/_{p\mathbb{Z}}$ ssi $p \equiv 1 \pmod 4$ p 5

:R] 57 **Appli 42 :** (Théorème des deux carrés)
Soit p premier. p est la somme de deux carrés ssi $p = 2$ ou $p \equiv 1 \pmod 4$

B] 38 **Prop 43 :** L'application $x \longmapsto \left(\frac{x}{p}\right)$ est multiplicative : $\forall x, x' \in \mathbb{Z}$, $\left(\frac{x}{p}\right)\left(\frac{x'}{p}\right) = \left(\frac{xx'}{p}\right)$.

.B] 139 VP **Thm 44 :** (Loi de réciprocité quadratique)
Si p, q premiers impairs, $p \neq q$, on a :
$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$$

Ex 45 : 15 est un carré modulo 17.

VP **Thm 46 :** (de Bachet)
Tout entier naturel s'écrit comme somme de 4 carrés.

UV] .73 .74 **Rq 47 :** Tous les entiers ne peuvent pas s'écrire comme la somme de trois carrés.
Aucun nombre de la forme $8n+7$ ne peut s'écrire comme la somme de trois carrés.

3) Équations diophantiennes

n] 73 75 **Déf 48 :** On appelle équation diophantienne une équation $P(X,Y,Z) = 0$ où les inconnues X, Y, Z sont des entiers et où P est un polynôme à plusieurs variables à coefficients entiers.

Prop 49 : $(x,y,z) \in \mathbb{N}^3$ est solution de l'équation de Diophante $x^2+y^2=z^2$ ssi $\exists d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$ premiers entre eux tels que (x,y,z) ou (y,x,z) soit égal à $(d(u^2-v^2), 2duv, d(u^2+v^2))$.

Thm 50 : (Sophie Germain)
Soit p premier impair tel que $q = 2p+1$ est premier. Il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tq $\begin{cases} xyz \not\equiv 0 \pmod p \\ x^p + y^p + z^p = 0 \end{cases}$ [XENS 1] p 167

4) Cryptographie

Système RSA :
On choisit deux "gros" nombres premiers p et q, $p \neq q$ [SP] p 90-91
Posons $n = pq$. $\varphi(n) = (p-1)(q-1)$
On choisit r tq $r \wedge \varphi(n) = 1$.
Notons $C : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $x \longmapsto x^r$ la fonction de codage.

Prop 51 : Sous ces hypothèses, on note $(u,v) \in \mathbb{Z}^2$ tq $ru + \varphi(n)v = 1$ ((u,v) existe car $r \wedge \varphi(n) = 1$).
Alors $C^{-1} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $x \longmapsto x^u$
autrement dit, $\forall x \in \mathbb{Z}$ $x^{ru} \equiv 1 \bmod n$.

Prop :
(✱) Soit $P \in \mathbb{F}_p[X]$ irréductible de degré r
$\mathbb{F}_p[X]/(P)$ est un corps à p^r éléments.

[illegible]

[PER] : Perrin – Cours d'algèbre

[RB] : Risler - Boyer – Algèbre pour la licence 3 : Groupes, anneaux, corps

[COM] : Combes - Algèbre et géométrie

[SP] : "Cours de calcul formel" Philippe Saux Picart
Algorithmes fondamentaux.

—. Loi de réciprocité quadratique .—
(via le symbole de Zolotarev)

JANVIER 2015

<u>Référence</u> : Algèbre pour la licence 3 ; Risler, Boyer.

<u>Théorème</u> : Pour p et q premiers distincts, on a

$$\left(\frac{p}{q}\right) = (1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$$

<u>Notation</u> : — ~~On fixe $n \in \mathbb{N}^*$, p un nombre premier, et m un entier premier avec n.~~

— Si s est une permutation d'un ensemble fini, on note $\varepsilon(s)$ sa signature.

— Si $n \in \mathbb{N}^*$, la multiplication par un entier m dans $\mathbb{Z}/n\mathbb{Z}$ est notée $\mu_n(m)$; et pour $k \in \mathbb{N}$, la translation par k dans $\mathbb{Z}/n\mathbb{Z}$ est notée $\tau_n(k)$.

<u>Rappel</u> : — La signature d'un cycle de longueur $k \in \mathbb{N}^*$ vaut $(-1)^{k-1}$.

— La signature d'une composée est le produit des signatures.

— On a $\varepsilon(\tau_n(1)) = (-1)^{n-1}$ car $\tau_n(1)$ est un cycle de longueur n ; et $\varepsilon(\tau_n(k)) = (-1)^{k(n-1)}$

car $\tau_n(k)$ est la composée, k fois, de $\tau_n(1)$.

— La signature d'une permutation est égale à $(-1)^l$ où l est le nombre d'inversion de cette permutation.

Définition : Pour $n \in \mathbb{N}^*$ et m premier avec n, le symbole de Zolotarev $e_n(m)$ est le nombre $\varepsilon(\mu_n(m))$.

Lemme (de Zolotarev). Pour p et q des nombres premiers impairs distincts, le symbol de Zolotarev est égal au symbole de Legendre :

$$\left(\frac{q}{p}\right) = e_p(q).$$

Démonstration. On note r l'ordre de q dans le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$. D'une part, $\mu_p(q)$ se décompose en cycle de longueur r, comme chacun de ces cycles est à support disjoint et que le support de $\mu_p(q)$ est $\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, il y a $\frac{p-1}{r}$ cycles. On a donc

$$e_p(q) = (-1)^{(r-1)\frac{p-1}{r}}.$$

D'autre part, d'après la proposition 40 du plan, on a $\left(\frac{q}{p}\right) \equiv x^{\frac{p-1}{2}} \mod p$. On compare ces expressions selon la parité de r :

— si r est pair, $m^{\frac{p-1}{2}} = \left(m^{\frac{r}{2}}\right)^{\frac{p-1}{r}}$ (on a bien $2|r$ et $r|p-1$)

$$\equiv (-1)^{\frac{p-1}{r}} \mod p$$
$$= (-1)^{(r-1)\frac{p-1}{r}} \quad \text{car } r-1 \text{ impair};$$

p premier $\Rightarrow \mathbb{Z}/p\mathbb{Z}$ intègre
$\Rightarrow m^{r/2} = \pm 1$
$\Rightarrow m^{r/2} = 1$ car r est l'ordre

— si r impair, $r \wedge 2 = 1$ et donc $2r \mid p-1$,
il vient $m^{\frac{p-1}{2}} = (m^r)^{\frac{p-1}{2r}} \equiv 1^{\frac{p-1}{2r}} \mod p$

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

car $\frac{p-1}{r}$ est pair.

<u>Démonstration</u> (du théorème) : On fixe p et q des nombres premiers impairs distincts. On note σ (resp. ρ) la permutation de $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ définie par

$$(i,j) \mapsto (qi+j, j)$$
$$(\text{resp. } (i,j) \mapsto (i, pj+i)).$$

(permutations car $q \in \mathbb{Z}/p\mathbb{Z}^*$. $p \in \mathbb{Z}/q\mathbb{Z}^*$)

Montrons que $\varepsilon(\sigma) = e_p(q)$ et $\varepsilon(\rho) = e_q(p)$. Pour $j \in \mathbb{Z}/q\mathbb{Z}$ on note σ_j la restriction de σ à $\mathbb{Z}/p\mathbb{Z} \times \{j\}$ prolongée à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par l'identité. La permutation σ peut être vu comme la composée des σ_j, $j \in \mathbb{Z}/q\mathbb{Z}$, et pour tout $j \in \mathbb{Z}/q\mathbb{Z}$ on a

$$\sigma_j = (\tau_p(j) \circ \mu_p(q), \ id) \quad \text{(notée en composante)}$$

d'où

$$\varepsilon(\sigma_j) = e_p(q) \times (-1)^{j(n-1)} = e_p(q) \quad \text{car } n \text{ impair}$$

et ainsi $\varepsilon(\sigma) = e_p(q)^q = e_p(q)$ car q impair
Par symétrie on a , $\varepsilon(\rho) = e_q(p)$.

Soit maintenant $\pi : \mathbb{Z}/pq\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

$$\overline{x} \longmapsto (\overline{x}^p, \overline{x}^q)$$

qui est un isomorphisme d'après le théorème chinois.
Et soit λ la permutation de $\mathbb{Z}/pq\mathbb{Z}$ définie par

– [soit $\bar{x} \in \mathbb{Z}/pq\mathbb{Z}$, $x = tpq + \underbrace{\tilde{r}}_{0 \leq \ < pq} = tpq + \tilde{t}q + \tilde{r}$ ← $0 \leq \ < q$]

$\tilde{t}$: $< p$ (car $\tilde{t} < pq$) et ≥ 0 $\Rightarrow \lambda$ bien déf avec $0 \leq i < p$, $0 \leq j < q$

$qi + j \mapsto pj + i$. Montrons que l'on a
$$\varepsilon(\lambda) = (-1)^{p(p-1)q(q-1)/4} .$$

~~Commençons par montrer les équivalences~~

$$\cancel{qi + j < qi' + j' \iff (i,j) <_{lex} (i',j')}$$

~~et~~ $\cancel{pj + i' < pj' + i' \iff (i,j) <_{lex^{-1}} (i',j')}$.

~~pour i et j dans $\mathbb{N}$. On rappelle que~~

$$\cancel{(i,j) <_{lex} (i',j') \iff \begin{cases} i < i' \\ \text{ou } i = i' \text{ et } j < j' \end{cases}}$$

~~Et on remarque~~ ~~On a~~

$$\cancel{pi + j < pi' + j \iff m(i - i') < j' - j}$$

Commençons par montrer l'équivalence
$$qi + j < qi' + j' \iff (i,j) <_{lex} (i',j')$$
$$\text{i.e. } \begin{cases} i < i' \\ \text{ou } i = i' \text{ et } j < j' \end{cases}$$

pour $i \in \{0, \dots, p-1\}$ et $j \in \{0, \dots, q-1\}$. On a
$$qi + j < qi' + j' \iff q(i - i') < j' - j$$

— Si $i > i'$ alors $i - i' > 0$ (donc $i - i' \geq 1$) et $q.(i - i') \geq q$. Or $j' - j < q$, ce cas est donc impossible.

— Si $i = i'$, il faut immédiatement $j < j'$.

— Sinon $i < i'$.

Par symétrie on a aussi
$$pj + i < pj' + i' \iff (i,j) <_{lex^{-1}} (i',j')$$
$$\iff (j,i) <_{lex} (j',i') .$$

Grâce à ces équivalences, il suffit, pour compter les inversions de λ, de compter le nombre de de couple $((i,j),(i',j'))$ de $\left([0,\dots,p-1]\times[0,\dots,q-1]\right)^2$ tel que

$$(i,j) <_{lex} (i',j') \quad \text{et} \quad (i',j') <_{lex^{-1}} (i,j).$$

$$\Leftrightarrow \begin{cases} i<i' \\ \text{ou } i=i' \text{ et } j<j' \end{cases} \quad \text{et} \quad \begin{cases} j'<j \\ \text{ou } j=j' \text{ et } i'<i \end{cases}$$

$$\Leftrightarrow \quad i<i' \quad \text{et} \quad j'<j$$

Il y en a donc $\binom{p}{2}\binom{q}{2} = \frac{p(p-1)\,q(q-1)}{4}$ et on obtient le résultat souhaité.

Il nous suffit maintenant de remarquer que

$$\lambda \circ \pi^{-1} \circ \sigma = \pi^{-1} \circ \rho .$$

puisque

$$\pi(\overline{qi+j}) = (\overline{qi+j}^{\,p}, \overline{j}^{\,q}) \text{ et}$$
$$\pi(\overline{i+pj}) = (\overline{i}^{\,p}, \overline{i+pj}^{\,q}) .$$

On en déduit, en prenant les signatures après avoir composé avec π dans les 2 membres

$$(-1)^{p(p-1)q(q-1)/4}\, e_p(q) = e_q(p)$$

On conclut grâce au lemme.

Théorème des quatres carrés

(énoncé par BACHET en 1621,
démontré par LAGRANGE 1772.)

JANVIER 2015

<u>Référence</u> : Oraux X-ENS, Algèbre 1 ; p. 149
ou Théorie des nombres ; D. Duverney ; p. 73.

<u>Théorème</u> : Tout entier naturel s'écrit comme somme de quatre carrés d'entier.

<u>Démonstration</u> : Commençons par énoncer l'identité suivante :

$$(*) \quad (a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = A^2+B^2+C^2+D^2$$

$$\text{où } \begin{cases} A = ax+by+cz+dt \\ B = ay-bx-ct+dz \\ C = az+bt-cx-dy \\ D = at-bz+cy-dx \end{cases}$$

pour tout $(a,b,c,d,x,y,z,t) \in \mathbb{Z}^8$; qui nous permet d'affirmer que si deux entiers sont somme de quatre carrés, alors leur produit aussi. Ainsi, pour montrer que tout entier, différent de 0 et 1, est somme de quatre carrés, il suffit, grâce au théorème de décomposition en facteurs premiers, d'établir le résultat pour tout nombre premier. Comme

$$2 = 1^2 + 1^2 + 0^2 + 0^2,$$

il suffit de le montrer pour tout nombre premier impair.

Soit p un nombre premier impair et soit E l'ensemble des entiers non nuls tels que np soit somme de quatre carrés. On souhaite montrer que $1 \in E$.

Tout d'abord, E n'est pas vide. On utilise le fait que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est somme de deux carrés[1]. En particulier, $\overline{-1}$ l'est, et il existe $(a,b) \in \mathbb{Z}^2$ tel que

$$-1 \equiv a^2 + b^2 \mod p$$

i.e. $0^2 + 1^2 + \alpha^2 + \beta^2 \equiv 0 \mod p.$

Comme $E \subset \mathbb{N}^*$ et non vide, on peut considérer son plus petit élément, que l'on note m.

Montrons que $m < p$. Soient $n \in \mathbb{N}^*$ et $(\alpha,\beta) \in \mathbb{Z}^2$ tels que

$$np = 1 + \alpha^2 + \beta^2 .$$

Quitte à changer n, on peut supposer que

$$|\alpha| < \frac{p}{2} \quad \text{et} \quad |\beta| < \frac{p}{2} .$$

En effet, comme p est impair on peut considérer $(\tilde{\alpha}, \tilde{\beta}) \in \mathbb{Z}^2$ tel que

$$\begin{cases} \alpha \equiv \tilde{\alpha} \mod p \\ \beta \equiv \tilde{\beta} \mod p \end{cases} \quad \text{et} \quad \begin{cases} |\tilde{\alpha}| < \frac{p}{2} \\ |\tilde{\beta}| < \frac{p}{2} \end{cases}$$

[p impair permet de mettre des inégalités strictes. On peut toujours choisir un représentant u avec $-\lfloor \frac{p-1}{2} \rfloor \leq u \leq \lfloor \frac{p}{2} \rfloor$]

On a alors

$$1 + \tilde{\alpha}^2 + \tilde{\beta}^2 \equiv 1 + \alpha^2 + \beta^2 \equiv 0 \mod p,$$

[1] Démontré à la fin.

et il existe $\tilde{n} \in \mathbb{N}^*$ tel que

$$1 + \tilde{\alpha}^2 + \tilde{\beta}^2 = \tilde{n} p.$$

On suppose donc que l'on a lesdites inégalités. Il vient

$$np = 1 + \alpha^2 + \beta^2 < \frac{p^2}{2} + 1$$

Ceci implique $n < p$ et donc $m < p$.

Montrons que m est impair. Par l'absurde, supposons m pair. Alors mp est pair et si on écrit

$$mp = a^2 + b^2 + c^2 + d^2,$$

on doit avoir a^2, b^2, c^2 et d^2 (et donc a, b, c et d), soit tous pairs, soit tous impairs, soit 2 de chaque parité. Dans ce dernier cas, on suppose que a et b sont pairs (et c et d impairs). Dans tous les cas, les entiers $a+b$, $a-b$, $c+d$, et - sont pairs et on a (en utilisant $u^2 + v^2 = \frac{1}{4}(u+v)^2 + \frac{1}{4}(u-v)^2$)

$$\frac{m}{2} p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2$$

c'est-à-dire $\frac{m}{2} \in E$, contradiction.

Montrons maintenant, également par l'absurde, que $m = 1$. Supposons $m > 1$ et conservons

$$mp = a^2 + b^2 + c^2 + d^2.$$

On considère les résidus de a, b, c et d modulo m, de valeur minimale (strictement inférieure à $\frac{m}{p}$ car m impair), que l'on note respectivement x, y, z, t. On a

$$x^2 + y^2 + z^2 + t^2 \equiv a^2 + b^2 + c^2 + t^2 \equiv 0 \mod m.$$

et x, y, z, t sont non tous nuls. En effet, s'ils étaient, m diviserait a, b, c et d, on aurait m^2 divise mp et donc $m \mid p$; ce qui est absurde si $m > 1$.
L'entier

$$m' = (x^2 + y^2 + z^2 + t^2)/m$$

est donc non nul. Nous allons montrer que $m' \in E$.
On a, avec $(*)$,

$$\begin{aligned} m^2 m' p &= (a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) \\ &= A^2 + B^2 + C^2 + D^2 \end{aligned}$$

où

$$\begin{aligned} A &= ax + by + cz + dt \equiv a^2+b^2+c^2+d^2 \equiv 0 \bmod m \\ B &= ay - bx - ct + dz \equiv ab - ba - cd + dc \\ &\equiv 0 \bmod m \\ &\equiv C \equiv D \bmod m. \end{aligned}$$

D'où

$$m' p = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2 .$$

Or $m' < m$ car

$$x^2 + y^2 + z^2 + t^2 < 4\left(\frac{m}{2}\right)^2 = m^2 .$$

Le fait que $m' \in E$ contredit donc la définition de m et on conclut que $m = 1$. Donc p est somme de quatre carrés.

Démontrons maintenant que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est somme de deux carrés. Soit $u \in \mathbb{Z}/p\mathbb{Z}$. Comme il y a exactement $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$ [1], on a

$$\mathrm{Card}\,\{x^2,\ x \in \mathbb{Z}/p\mathbb{Z}\} = \mathrm{Card}\,\{u - y^2,\ y \in \mathbb{Z}/p\mathbb{Z}\} = \frac{p+1}{2} .$$

En utilisant la formule $\# A \cup B = \# A + \# B - \# A \cap B$, on en déduit que leur intersection est non vide, ce qui permet de conclure.

[1] $\# {}^2\mathbb{Z}/p\mathbb{Z} = \#\{\text{carrés non nuls}\} + 1 = \frac{p-1}{2} + 1 = \frac{p+1}{2}$

$$\mathrm{Im}\,\phi = \{\text{carrés non nuls}\} \simeq \underbrace{\left(\mathbb{Z}/p\mathbb{Z}^*\right)/\{\pm \bar{1}\}}_{= \{\{\pm a\},\ a \in \mathbb{Z}/p\mathbb{Z}^*\}} = \left(\mathbb{Z}/p\mathbb{Z}^*\right)/\mathrm{Ker}\,\phi$$

où $\phi : \mathbb{Z}/p\mathbb{Z}^* \to \mathbb{Z}/p\mathbb{Z}^*$, $x \mapsto x^2$.