I [120] Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

I Structure de $\mathbb{Z}/n\mathbb{Z}$ [P]

1) Les anneaux $\mathbb{Z}/n\mathbb{Z}$

def 1: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est le quotient de $(\mathbb{Z}, +, \times)$ par l'idéal $n\mathbb{Z}$.

Rq 2: on identifiera $m \in \mathbb{Z}$ avec $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ lorsque le contexte est clair.

prop 3: $(\mathbb{Z}/n\mathbb{Z}, +)$ est à isomorphisme près l'unique groupe monogène à n éléments.

Thm 4: Soit $m \in \mathbb{Z}/n\mathbb{Z}$; $\langle m \rangle = \mathbb{Z}/n\mathbb{Z} \Leftrightarrow m \wedge n = 1 \Leftrightarrow m \in (\mathbb{Z}/n\mathbb{Z})^\times$

ex 5: Le groupe $\mathbb{U}_n$ des racines n^{e} de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, et ses générateurs sont les $e^{2i\pi k/n}$ avec $k \wedge n = 1$

def 6: [Indicatrice d'Euler]
$\varphi : n \longmapsto \mathrm{Card}(\{1 \leq m \leq n,\ m \wedge n = 1\})$

ex 7: si p premier, $\varphi(p) = p-1$

prop 8: [Théorème d'Euler]
Soit $n \in \mathbb{N}$, $a \in \mathbb{N}$ $\quad a \wedge n = 1 \Leftrightarrow a^{\varphi(n)} \equiv 1\ [n]$

prop 9: Si $m \wedge n = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$

ex 10: $42^{40} \equiv 1\ [55]$

Thm 11: $\sum_{d|n} \varphi(d) = n$

2) Étude algébrique

Prop 12: $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier.

Prop 13: Pour $d | n$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d : $\{k \frac{n}{d},\ 0 \leq k \leq d-1\}$. $\mathbb{Z}/n\mathbb{Z}$ n'a pas d'autres sous-groupes.

ex 14: étude des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$

Prop 15: Les idéaux de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$

Thm 16: $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Prop 17: $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$
a est un nilpotent de $\mathbb{Z}/n\mathbb{Z}$ ssi $p_1 \cdots p_r | a$
Il y a donc $(p_1^{\alpha_1 - 1}) \cdots (p_r^{\alpha_r - 1})$ nilpotents.

ex 18: Les nilpotents de $\mathbb{Z}/36\mathbb{Z}$ sont 0, 6, 12, 18, 24 et 30

Prop 19: $\mathrm{Card}(\mathrm{Hom}_{gp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})) = m \wedge n$

3) Le théorème chinois [SP]

Thm 20: Si $m \wedge n = 1$, alors $(\mathbb{Z}/mn\mathbb{Z}) \underset{\text{anneaux}}{\approx} (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$

Rq 21: Si $m \wedge n > 1$, l'ordre d'un élément de $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ est au plus $m \vee n\ (\neq mn)$, donc ce groupe n'est pas monogène.

Corollaire 22: Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, alors il y a 2^r idempotents dans l'anneau $(\mathbb{Z}/n\mathbb{Z})$.

Application 23:
Le système de congruence $\begin{cases} x \equiv a_1\ [k_1] \\ \vdots \\ x \equiv a_r\ [k_r] \end{cases}$ a des solutions (unique modulo $k_1 \vee k_2 \vee \cdots \vee k_r$)
ssi pour $i \neq j$, $a_i - a_j \equiv 0\ [k_i \wedge k_j]$

Rq 24: si les k_i ne sont pas premiers entre eux, on fait une réduction :
$\begin{cases} x \equiv a_1\ [k_1] \\ x \equiv a_2\ [k_2] \end{cases} \Leftrightarrow \begin{cases} x \equiv a_1\ [k_1/(k_1 \wedge k_2)] \\ x \equiv a_2\ [k_2] \end{cases}$ si $a_1 - a_2 \equiv 0\ [k_1 \wedge k_2]$

méthode naïve 25: calcul de la préimage de $(0, \ldots, 0, 1, 0, \ldots, 0)$ (i^e position) par l'isomorphisme du théorème chinois.
$\rightarrow$ si $a = [k_1 \cdots k_{i-1} k_{i+1} \cdots k_r]^{-1}[k_i]$, donnée par $a \hat{k}_i$ (modulo le produit des k_j)

[SP] $p = 2$ / Rq 24

Algorithme de Garner (26):
Un autre isomorphisme est donné par $\begin{array}{l} \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_r\mathbb{Z} \longrightarrow \mathbb{Z}/k_1 \cdots k_r\mathbb{Z} \\ (\nu_1, \ldots, \nu_r) \longmapsto \nu_1 + \nu_2 k_1 + \cdots + \nu_r k_1 k_2 \cdots k_{r-1} \end{array}$
On pose donc $x \equiv \nu_1 + \cdots + \nu_r k_1 \cdots k_{r-1}\ [k]$ et on veut déterminer les ν_i :
- $\nu_1 \equiv a_1\ [m_1]$
- $k_1 \cdots k_{i-1}$ est inversible d'inverse K modulo k_i ;
$\nu_i \equiv K(a_i - \nu_1 - \nu_2 k_2 - \cdots - \nu_{i-1} m_1 \cdots m_{i-2})\ [m_i]$

$\rightarrow$ même complexité asymptotique : $O(r \log^2(\prod_i k_i))$,
mais plus efficace en pratique, et stable par ajout de contraintes.

Ex 27: Calcul de la solution de $\begin{cases} x \equiv 8\ [11] \\ x \equiv 3\ [17] \\ x \equiv 5\ [42] \end{cases}$ par les deux méthodes.

Application 28: Légende des calculs des pertes de l'armée chinoise.

II Applications en arithmétique

1] Carrés de $(\mathbb{Z}/n\mathbb{Z})^\times$:

[Perrin] III.2.d

a] Cas où n est premier :

Def 29 : Si p premier impair, $a \in \mathbb{Z}$, on note $\left(\frac{a}{p}\right) = \begin{cases} a^{\frac{p-1}{2}} \text{ si } a \wedge p = 1 \\ 0 \text{ sinon} \end{cases}$ le symbole de Legendre de a dans p.

Thm 30 :
- $\forall a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $\forall q$ premier impair, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ssi } \overline{a} \text{ est un carré dans } (\mathbb{Z}/p\mathbb{Z})^\times \\ 0 & \text{ssi } p \mid a \end{cases}$.

Appl 31 : Il y a $\frac{p-1}{2}$ carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Rq 32 : Si $p=2$, $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ contient 1 carré.

b] Cas où $n = p^\alpha$ (p premier)

[Hindry] VII.3.8 [Serre] II.2.2

Lemme (de Hensel) 33 : Soient $P \in \mathbb{Z}[X]$, $x_0 \in \mathbb{Z}$, $n \in \mathbb{N}^*$, $k \in \mathbb{N}$ tels que $k < \frac{n}{2}$, $P(x_0) \equiv 0 \ [p^n]$, et $P'(x_0) = p^k b$ avec $p \nmid b$. Alors $\exists (x_i)_{i \in \mathbb{N}} \subset \mathbb{Z}$ tels que $\forall i$, $x_{i+1} \equiv x_i \ [p^{n+i-k}]$ et $P(x_i) \equiv 0 \ [p^{n+i-k}]$.

Cor 34 :
- Si $p \neq 2$, alors $\forall \alpha \geq 1$, $\left(a \in \left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^{\times 2}\right) \Leftrightarrow \left(a \bmod p \in \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times 2}\right)$
- Si $p=2$, alors $\forall \alpha \geq 3$, $\left(a \in \left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^{\times 2}\right) \Leftrightarrow (a \equiv 1 \ [8])$

Rq 35 : 1 est le seul carré de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$.

c] Cas n quelconque :

[?]

Prop 36 : Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ la décomposition de n en fact. premiers. Alors $a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times 2} \Leftrightarrow \forall i \in [\![1,k]\!]$, $a \in \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^{\times 2}$

Cor 37 : $\operatorname{card}\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times 2}\right) = \prod_{i=1}^{k} \frac{p_i - 1}{2} p_i^{\alpha_i - 1}$ (si n impair)

Rq 38 : On a, pour $\alpha \geq 3$, $\operatorname{card}\left(\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^{\times 2}\right) = 2^{\alpha-3}$.

Def 39 : Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et a impairs. Alors le symbole de Jacobi de a sur n est $\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}$

Prop 40 : Si a, b et n sont impairs, alors on a :
- $\left(\frac{a}{n}\right) = 0$ ssi $a \wedge n \neq 1$.
- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
- $\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)(-1)^{\frac{n-1}{2}\frac{a-1}{2}}$

Appl 41 : Si $p = x^2 - 6y^2$ est premier, alors $p \equiv 1, 5, 19$ ou $23 \ [24]$

2] Quelques équations diophantiennes :

[Hindry] I.3.6

a] Sommes de carrés : [Hindry] III.1 p76

On s'intéresse aux équations de la forme $\sum_{i=1}^{k} x_k^2 = n$

Thm (des 2 carrés) 42 : Soit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Alors l'équation $n = x_1^2 + x_2^2$ a une solution si et seulement si $\forall i \in [\![1,r]\!]$, $(p_i \equiv 3 \ [4] \Rightarrow \alpha_i \text{ est pair})$.

Thm (des 4 carrés) 43 : Pour tout $n \in \mathbb{N}$, l'équation (DEV) $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ a une solution. [FGN] p.148

Comptage des solutions : [Hindry] III.6.11 p118

Thm 44 : Soit $r_k(n) = \operatorname{card}\left\{(x_1, \dots, x_k) \in \mathbb{Z}^k / \sum_{i=1}^{k} x_i^2 = n\right\}$.
Si $d_i^{(n)} = \operatorname{card}\{d \in \mathbb{N} / d \mid n \text{ et } d \equiv i \ [4]\}$ et $d_3^{(n)} = \operatorname{card}\{d \in \mathbb{N} / d \mid n \text{ et } d \equiv 3 \ [4]\}$ alors
- $r_2(n) = 4(d_1(n) - d_3(n))$
- $r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d$ (Identité de Jacobi)

b] Équation de Fermat [Hindry] III.2 p81

Thm 45 (Fermat-Wiles) : Si $n \geq 3$, les solutions de $x^n + y^n = z^n$ satisfont $xyz = 0$. (Admis)

Prop 46 : (Cas $n=2$) Les solutions de $x^2 + y^2 = z^2$ sont de la forme (quitte à échanger x et y) $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$ pour u et v premiers entre eux.

Thm 47 : (Cas $n=4$) Il n'y a pas de solutions à $x^4+y^4=z^4$ sauf si $xyz=0$.

DEV

[FGN] p153 **Thm 48** : (Sophie Germain) Si p et $2p+1$ sont premiers, alors les solutions de $x^p+y^p=z^p$ satisfont $xyz \equiv 0\ [p]$

3] Progression arithmétique :

Thm 49 : (Dirichlet) Si $a \wedge b = 1$, alors il existe une infinité de nombres premiers congrus à a modulo b (Admis)

Thm 50 : (Cas $a=1$) Pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers de la forme $nk+1$.

4] Test de primalité

Rappel 51 : [petit théorème de Fermat ; prop 9 avec n premier] Si p est premier, alors pour $a \in \{1, \dots, p-1\}$, $a^{p-1} \equiv 1\ [p]$

C-Ex 52 : 15 n'est pas premier, pourtant $4^{14} \equiv 1\ [15]$

- $341 = 11 \times 31$, et $2^{340} \equiv 1\ [341]$

Déf 53 : Un nombre n est dit **de Carmichael** s'il n'est pas premier mais que pour $a \in \{1, \dots, n-1\}$, $a^{n-1} \equiv 1\ [n]$

Ex 54 : $561 = 11 \times 51$ est un nombre de Carmichael.

Thm 55 [admis] : Il existe une infinité de nombres de Carmichael

[SAF] p184 **Rq 56** : Si $C(n) = \{k \leq n,\ k \text{ est de Carmichael}\}$, $\pi(n) = \{k \leq n,\ k \text{ premier}\}$, $C(n) = o(\pi(n))$ $n \to \infty$

[SPR] p.73 **Prop 57** : Soit $n \in \mathbb{N}$. S'il existe $a < n$, $a \wedge n = 1$ tel que $a^{n-1} \neq a\ [n]$, alors

$$\left| \left\{ a < n,\ a \wedge n = 1,\ a^{n-1} \neq a\ [n] \right\} \right| > \frac{\varphi(n)}{2}$$

Test de Miller-Rabin faible (58)

entrée : n, k

algo : (faire k fois : prendre $a \in \{1, \dots, n-1\}$, si $a \wedge n \neq 1$ ou $a^{n-1} \neq a\ [n]$, finir et $\to$ non) $\to$ oui

Rq 59 : Si $\to$ non, n n'est pas premier

si $\to$ oui, n a une probabilité $\geq 1 - \frac{1}{2^k}$ d'être premier ou de Carmichael.

pour $k=10$, on a un test de primalité fiable à 99%

[SAF] p185 **Thm 60** : [Lucas-Lehmer]

Soit $n \in \mathbb{N}$. S'il existe $1 < a < n$ tel que pour p premier, $p \mid (n-1)$, $a^{n-1} \equiv 1\ [n]$ et $a^{(n-1)/p} \neq 1\ [n]$, alors n est premier

[SAF] p189 **Rq 61** : On peut à l'aide de ce test rajouter un calcul peu coûteux au test de Miller-Rabin pour changer la constante $\frac{1}{2} \to \frac{1}{4}$

[SAF] p185 **Rq 62** : Si s est premier, $M_s = 2^s - 1$; soit $1 < a < M_s$ avec $(a^{\frac{s-1}{4}})^4 = 1$ (ex : $a=4$)

Soit $L : \mathbb{N} \to \mathbb{N}$, $L_1 := a$ et $L_{i+1} := L_i^2 - 2$;

alors $L_{s-1} \equiv 0\ [M_s] \iff M_s$ est premier

Rq 63 : Les plus grands nombres premiers connus à ce jour ont été découverts avec cette méthode (ex : $2^{74\,207\,281} - 1$)

5] Cryptographie [SP] p 90 → 96

Lemme 64 : Soient p, q premiers, $n = pq$, $\varphi(n) = (p-1)(q-1)$

Si $t \equiv 1\ [\varphi(n)]$ alors pour $1 \leq a < n$, $a^t \equiv a\ [n]$

Cryptage RSA : (65) (On note $n = a\%b$ pour $a \equiv n\ [b]$ et $0 \leq n \leq b-1$)

p, q deux nombres premiers "grands"

$e \in \{1, \dots, n\}$ tq $e \equiv 1\ [\varphi(n)]$ $(e \neq 1)$ $\quad d := e^{-1}\ [n]$

(e, n) clé publique, $(d, \varphi(n))$ clé privée.

Pour m message code, $M \equiv m^e \%\, n$ message crypté.

grâce au lemme, $M^d \equiv m\ [n]$ donc $M^d \%\, n = m$

Rq 66 : On peut utiliser l'exponentiation rapide.

Rq 67 : Si Alice et Bob ont comme clés publiques (e_a, n_a), (e_b, n_b) et comme clés privées d_a et d_b, alors par $M = (m^{e_a} \%\, n_a)^{d_b} \%\, n_b$, Bob peut envoyer un message à Alice l'assurant qu'il est bien l'expéditeur

Rq 68 : Si $n_a = n_b$, on peut décoder leur conversation à l'aide d'une relation de Bézout.

[P.] [Perrin] Le Perrin©

[SP] Philippe Saux-Picart, "Cours de calcul formel, Algorithmes fondamentaux", ellipses.

[Hindry] Marc Hindry, "Arithmétique", Calvage & Mounet.

[Serre] Jean-Pierre Serre, "Cours d'arithmétique", PUF, 4e édition.

[FGN] Oraux X-ENS algèbre 1, 2e édition.

[SAF] Sabah Al Fakir, "Algèbre et théorie des nombres, Cryptographie, primalité", ellipses

[SPR] P. Saux-Picart, Éric Rannou, "Cours de calcul formel, Systèmes polynomiaux, applications", ellipses.

Dév. possibles :

* Réciprocité quadratique via Sommes de Gauss
* Thm des 2 carrés (via $\mathbb{Z}[i]$, .. justifier le lien ac $\mathbb{Z}/n\mathbb{Z}$)
* Identité de Jacobi ? (Thm 44)
* Fermat pour $n=2$ et 4
* Thm de Dirichlet

① PR φ est multiplicative ? $m \wedge n$

$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ => puis [illegible] !

② $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$?

③ $\varphi(n) = \prod (p_i - 1) p_i^{\alpha_i - 1}$

④ $\sum_{d|n} \varphi(d) = n$ → pour $n = p^\alpha$ ok

→ pour n [illegible] avec [illegible].

⑤ $(\mathbb{Z}/n\mathbb{Z})^*$ cyclique ?

⑥ $(\mathbb{Z}/8\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

⑦ $x \equiv 3\ [13]$ et $x \equiv 7\ [19]$ Résoudre.

$\mathbb{Z}/247\mathbb{Z} \simeq \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z}$

$x \longleftarrow (3, 7)$

$3 \times 13 \longrightarrow (0, 1)$

$19 \times (-2) \longrightarrow (1, 0)$

$19 = 13 \times 1 + 6$

$13 = 6 \times 2 + 1$

$1 = 13 - 6 \times 2 = 13 - (19 - 13) \times 2$

$1 = 13(3) - 2 \times 19$

$x = 3 \times 7 \times 13 + 3 \times (-2) \times 19$

unique sol dans $\mathbb{Z}/247\mathbb{Z}$

⑧ $\mathbb{Z}/p\mathbb{Z}^\times \longrightarrow \mathbb{Z}/p\mathbb{Z}^\times$, $x \longmapsto x^k$ CNS pour bijection => premier avec $(p-1)$.

$SL_2(\mathbb{Z}/3\mathbb{Z})$.

=> $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/n\mathbb{Z})$.

X-ENS al 2.

=> ⚠ Le théorème est partout donc à le mettre au début.

Théorème des 4 carrés

Admis : (sauf si temps ou rab) : thm des 2 carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Thm : Soit $n \in \mathbb{N}$. Il existe $a,b,c,d \in \mathbb{N}$ tq
$n = a^2+b^2+c^2+d^2$.

Soit $E = \{n \in \mathbb{N} / \exists a,b,c,d,\ n = a^2+b^2+c^2+d^2\}$

Pour $a,b,c,d,x,y,z,t \in \mathbb{N}$, on remarque
$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = A^2+B^2+C^2+D^2$
avec $A = ax+by+cz+dt$ (⁂)
$B = ay-bx-ct+dz$
$C = az+bt-cx-dy$
$D = at-bz+cy-dx$
donc si $m,n \in E$, alors $mn \in E$.

0, 1, 2 sont dans E, on va donc montrer
si p premier impair, $p \in E$.

Soit p premier impair. $E_p = \{n \in \mathbb{N},\ np \in E\}$
montrons $1 \in E_p$.

1ère étape : il existe $n < p$ tq $n \in E_p$

par le théorème des deux carrés, il existe α, β tel que
$\alpha^2+\beta^2 \equiv -1\ [p]$
càd $\exists n \in \mathbb{N},\ \alpha^2+\beta^2+1^2+0^2 = np$.

Pour m impair, $\varphi_m : \mathbb{N} \longrightarrow \mathbb{Z}$
$x = am+b \mapsto$ b si $b < \frac{m}{2}$, $b-m$ sinon
↑ division euclidienne par m.

$\forall x,\ \varphi_m(x) \equiv x\ [m]$
$|\varphi_m(x)| < \frac{m}{2}$

Alors $\varphi_p(\alpha)^2 + \varphi_p(\beta)^2 + 0^2 + 1^2 = n'p$ donc $n' \in E_p$

et $n'p \leqslant 2\left(\frac{p}{2}\right)^2 + 1 < p^2$ d'où $n' < p$

2e étape : Soit $m = \min(E_p)$; on a $m = 1$ par l'absurde

- si m est pair, on a $mp = a^2 + b^2 + c^2 + d^2$, parmi a, b, c, d soit 4 pairs, soit 2 pairs (a et b) et 2 impairs (c et d), soit 4 impairs

alors $(a-b)$, $(a+b)$, $(c-d)$ et $(c+d)$ sont pairs, et

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

ce qui contredit la minimalité de m

- si m impair > 1, alors, $mp = a^2 + b^2 + c^2 + d^2$

soient $\begin{cases} x = \varphi_m(a) \\ y = \varphi_m(b) \\ z = \varphi_m(c) \\ t = \varphi_m(d) \end{cases}$ alors $x^2 + y^2 + z^2 + t^2 \equiv 0 \ [m]$

soit $m = \frac{x^2+y^2+z^2+t^2}{m}$

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

$A = ax + by + cz + dt \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \ [m]$ $\quad C \equiv 0 \ [m]$

$B = ay + bx - ct + dz \equiv ab - ba - cd + dc \equiv 0 \ [m]$ de même $D \equiv 0 \ [m]$

alors $mp = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2$

ce qui contredit la minimalité de m

donc $m = 1$ et $E = \mathbb{N}$.

Théorème de Sophie Germain

Thm: Soit p premier tel que $2p+1=q$ soit aussi premier.
Il n'existe pas de $x,y,z \in \mathbb{Z}$ tels que $\begin{cases} x^p+y^p+z^p=0 \\ x,y,z \not\equiv 0 \ [p] \end{cases}$

Par l'absurde, soit (x,y,z) un tel triplet.

- Si $x \wedge y = d \neq 1$, alors $d \mid x^p+y^p=-z^p$ d'où $d \mid z$

et $\left(\frac{x}{d}\right)^p+\left(\frac{y}{d}\right)^p+\left(\frac{z}{d}\right)^p=0$ nous fournit une autre solution
on peut donc supposer les x,y,z premiers entre eux.

- Il existe α, α tels que $\underbrace{y+z}_{=A}=\alpha^p$ et $\underbrace{\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k}_{B}=\alpha^p$

en effet, $AB=(y+z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = y^p+z^p=-x^p$

Si $A \wedge B = d \neq 1$, alors $y \equiv -z \ [d]$ donc $B \equiv \sum_{k=0}^{p-1} y^{p-1-k}y^k \equiv py^{p-1} \ [d]$
alors $d \mid x$
donc $d \mid p$ $\rightsquigarrow$ absurde car $p \nmid x$ et p premier
ou $d \mid x$ $\rightsquigarrow$ absurde car $y \wedge z = 1$

d'où $AB=-x^p$ et $A \wedge B = 1$ donc il existe a, α tq $A=a^p$ et $B=\alpha^p$

de même, on montre qu'il existe b, c tels que $x+z=b^p$
$x+y=c^p$

- Si $q \nmid m$, alors $m^p \equiv \pm 1 \ [q]$ $(*)$

en effet, $m^{q-1} \equiv 1 \ [q]$ et $m^{q-1} = m^{p^2}$

Si q ne divise ni x, ni y, ni z,

alors $b=x^p+y^p+z^p \equiv \begin{cases} 3 \\ -1 \\ 1 \end{cases}$ $[q]$: absurde.

par (*)

De plus, x, y, z sont premiers entre eux 2 à 2, donc

q divise l'un des trois : on peut supposer $q \mid x$

$-b^p + c^p - a^p = x+z+x+y-y+z = 2x \equiv 0 \ [q]$

$q \mid x$ donc $b^p \equiv y \equiv \pm 1 \ [q]$ et $c^p \equiv y \equiv \pm 1 \ [q]$

si $q \nmid a$, alors $b^p + c^p - a^p \equiv \begin{cases} -3 \\ -1 \\ 1 \end{cases}$ $[q]$: absurde

donc $q \mid a$.

donc $y+z-a \equiv 0 \ [q]$

d'où $x^p = \sum_{k=0}^{p-1} (-2)^{p-1-k} y^k \equiv p\, y^{p-1} \ [q]$

or $y \equiv \pm 1 \ [q]$ d'où $x^p \equiv p \ [q]$

or d'après (*), une puissance p^e est congrue à $0, -1$ ou 1 modulo q !

donc x, y, z ne peuvent exister.