Équation de Sophie Germain

Julie Parreaux

2018-2019

Référence du développement : X-ENS algèbre 1 [1, p.167]

Leçons où on présente le développement : 120 (Anneau $\mathbb{Z}/n\mathbb{Z}$) ; 126 (Équations arithmétiques).

1 Introduction

L'équation de Fermat est une des équations mathématiques des plus connues. Comme souvent sa résolution a demandé de nombreuses avancées mathématiques et dans notre cas même des avancées informatique. Ici on montre le théorème de Fermat dans un cas particulier. Cette preuve nous vient d'une mathématicienne Sophie Germain.

Sophie Germain (1776 - 1831) est quasiment a seule mathématicienne de son temps. Elle s'est formée par correspondance puisqu'elle n'était pas admise dans les écoles prestigieuse en tant que femme. Elle s'est alors attaqué au théorème de Fermat qu'elle a démontrer dans un cas particulier : pour les entier premier de Sophie Germain. Cependant ce résultat pour lequel elle a correspondu avec Gauss a été écrit sous son pseudonyme masculin.

2 Étude de l'équation de Sophie Germain

Définition. Soit p un nombre premier. p est appelé entier premier de Sophie Germain si $q = 2p + 1$ est premier.

Théorème. *Soit p un nombre premier de Sophie Germain. Alors, il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $x^p + y^p + z^p = 0$ et $xyz \not\equiv 0[p]$.*

Schéma du développement

Ce développement est très long, il est difficile (voire impossible) de tout faire : il faut faire des choix (ne pas faire tous les calculs).

1. En supposant que $\text{pgcd}(x, y, z) = 1$ et montrer que x, y, z sont premiers entre-eux.
2. Montrer qu'il existe trois entiers a, b et c tels que $y + z = a^p$, $x + y = c^p$ et $x + z = b^p$.
   (a) Montrer le lemme : si $u \wedge v = 1$ et $uv = x^p$, alors $u = a^p$ et $v = b^p$.
   (b) Montrer qu'il existe deux entiers a et α tels que $y + z = a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$.
   (c) Montrer qu'il existe b et c : par symétrie.
3. Montrer que $m^p \equiv \pm 1[q]$.
4. Montrer que $b^p + c^p - a^p \equiv 0[q]$, $a \equiv 0[q]$, $y \equiv c^p[q]$ et $\alpha^p \equiv py^{p-1}$.

Démonstration. Raisonnons par l'absurde : supposons qu'il existe $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0[p]$ et $x^p + y^p + z^p = 0$.

Étape 1 : montrons que $\text{pgcd}(x,y,z) = 1$ et que x, y, z sont premiers entre-eux. Aller vite sur cette partie.

- Soit $d = \overset{\circ}{pgcd}(x,y,z)$. Posons $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ et $z' = \frac{z}{d}$ (par les propriétés du pgcd, x', y' et z' sont dans $\mathbb{Z}$). On a alors, $x' + y' + z' = 0$ (on factorise par d l'équation précédente) et$x'y'z' \not\equiv 0[p]$ (par multiplication de $p^{-1} \not\equiv 0[p]$ et intégrité de l'anneau $\mathbb{Z}/p\mathbb{Z}$). On peut supposer que $\text{pgcd}(x,y,z) = 1$ (quitte à faire ce calcul).
- Montrons que x et y sont premiers entre eux. Raisonnons par l'absurde et supposons que $\text{pgcd}(x,y) > 1$. Notons p_c un diviseur premier de $\text{pgcd}(x,y)$ (existe par le théorème fondamental de l'arithmétique). Comme p_c divise $x^p + y^p$ (car p_c divise x et y par définition du pgcd). Le lemme d'Euclide implique que p_c divise z^p. Donc p_c divise $\text{pgcd}(x,y,z)$. Contradiction.
- Un raisonnement analogue pour les deux autres couples permet de montrer que x, y, et z sont premiers entre eux.

Étape 2 : montrons qu'il existe trois entiers a, b et c tel que $y + z = a^p$, $x + y = c^p$, $x + z = b^p$. On commence par énoncé un lemme.

Lemme ([1, p.140]). *Si $u \wedge v = 1$ et $uv = x^p$, alors $u = a^p$ et $v = b^p$.*

Démonstration. Par le théorème fondamental de l'arithmétique, on décompose $u = \prod_{p\in\mathcal{P}} p^{\alpha_p}$, $v = \prod_{p\in\mathcal{P}} p^{\beta_p}$ et $x = \prod_{p\in\mathcal{P}} p^{\gamma_p}$. Comme $uv = x^p$, pour tout p premier $\alpha_p + \beta_p = k\gamma_p$ (on considère x^k). De plus, $u \wedge v = 1$ (par hypothèse), donc pour tout p premier, $\alpha_p\beta_p = 0$. Donc pour tout entier p premier, k divise α_p et k divise β_p. Donc u et v sont donc des puissances $k^{\text{ième}}$. □

Étape a : montrons qu'il existe deux entiers a et α tels que $y + z = a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-h}y^h = \alpha^p$. On cherche alors à applique le lemme à $u = y + z$ et $v = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$.

- Montrons que $uv = (y+z)(\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k) = (-x)^p$. On a

$$\begin{array}{rcll} uv & = & (y+z)(\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k) & \text{(définition)} \\ & = & \sum_{k=0}^{p-1}(-1)^{p-1-k}(z)^{p-k}y^k + \sum_{k=0}^{p-1}(-1)^{p-1-k}(z)^{p-k-1}y^{k+1} & \text{(on développe par rapport à } (y+z)) \\ & = & z^p - \sum_{k=1}^{p-1}(-1)^{p-k}(z)^{p-k}y^k + \sum_{k=1}^{p-1}(-1)^{p-k}(z)^{p-k}y^k + z^p & \text{(on déconstruit la somme)} \\ & = & z^p + z^p & \text{(on simplifie)} \\ & = & -x^p = & (y^p + z^p + x^p = 0) \\ & = & (-x)^p & \text{(car } p \text{ est impaire)} \end{array}$$

- Montrons que $y + z$ et $\sum_{h=0}^{p-1}(-z)^{p-1-h}y^h$ sont premiers entre eux. Raisonnons par l'absurde et supposons qu'ils ont un co-diviseur premier p'.
  - Comme $uv = (-x)^p$, p'^2 divise $-x^p$ ($y + z = ap'$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = bp'$ (p' diviseur commun au deux) et donc $abp'^2 = (-x)^p$ en multipliant les deux valeurs). On en déduit que p' divise x.
  - Comme $y \equiv z[p']$ (car p' divise $y + z$ par hypothèse), on a

$$\begin{array}{rcll} \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k & \equiv & \sum_{k=0}^{p-1} y^{p-1}[p] & (\equiv \sum_{k=0}^{p-1}(-z)^{p-1-k}(-z)^k \equiv \sum_{k=0}^{p-1}(-z)^{p-1} \equiv \sum_{k=0}^{p-1} y^{p-1}) \\ & & & \text{(en appliquant deux fois la remarque)} \\ & \equiv & py^{p-1}[p] & \text{(somme indépendante de } k) \\ & \equiv & 0[p] & (p' \text{ diviseur de la somme}) \end{array}$$

    Donc p' divise py^{p-1}.
  - Par le lemme de Gauss, on a deux cas :

    Soit p' divise p Dans ce cas, $p' = p$ (car p est premier) et p divise x. Contradiction.

    Soit p' divise y^{p-1} Dans ce cas, p' divise y et $x \wedge y > 1$. Contradiction.
- Par ce qui précède, nous pouvons appliquer le lemme et on a alors l'existence de deux entiers α et a tels que $y + z = a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-h}y^h = \alpha^p$.

Étape b : montrons qu'il existe b et c. On raisonne par symétrie.

Étape 3 : montrons que $m^p \equiv \pm 1[q]$. Soit $m \in \mathbb{Z}$ tel que $q = 2p - 1$ ne divise pas m.

— Par le petit théorème de Fermat, on a $m^{q-1} \equiv 1[q]$ (q est premier). Comme $q = 2p - 1$, $(m^p)^2 \equiv 1[q]$. Donc $m^p \equiv 1[q]$ ou $m^p \equiv -1[q]$.

— Supposons par l'absurde qu'aucun des trois entiers x, y, z n'est divisible par q. Alors, on a $x^p \equiv \pm 1[q]$, $y^p \equiv \pm 1[q]$ et $z^p \equiv \pm 1[q]$. En sommant, on obtient $x^p + y^p + z^p \equiv a[q]$ où $a \in \{3, 1, -1, -3\}$. Contradiction car $q \leq 5$. Donc une des trois variables est divisible par q.

— On suppose sans perte de généralité x et $yz \equiv 0[q]$ (x, y et z sont deux à deux premier entre eux).

Étape 4 : montrons que $b^p + c^p - a^p \equiv 0[q]$, $a \equiv 0[q]$, $y \equiv c^p[q]$ et $\alpha^p \equiv py^{p-1}$.

— Par l'étape 2 : $y + z = a^p$, $x + y = c^p$ et $x + z = b^p$: $b^p + c^p - a^p = 2x \equiv 0[q]$.

— $y \equiv c^p[q]$ puisque $x \equiv 0[q]$.

— Comme q ne divise pas y et q et c. Donc $y \equiv \pm 1[q]$. De même $z \equiv \pm 1[q]$.

— Comme q ne divise pas a, $a^q \equiv \pm 1[q]$. On a alors, $c^p + b^p - a^p \equiv x[q]$ avec $x \in \{3, 1, -1, -3\}$. Donc q divise a.

— Comme $y + z \equiv a^p \equiv 0[q]$, $\alpha^p \equiv py^{p-1}[q]$ (calcul de la somme modulo p). Donc $z \equiv \pm 1[q]$. Donc $\alpha^p \equiv p(-1)^{p+1} \equiv p$. Absurde pour z.

Contradiction □

Références

[1] S.Nicolas S. Francinou, H. Gianella. *Oraux X-ENS, Algèbre 1*. Cassini.