PRÉPARATION À L'AGRÉGATION EXTERNE : NOMBRES DE SOPHIE GERMAIN

TONY LIMAGNE

1. Préliminaires

Lorsque $n \geqslant 2$ est un entier et p est un nombre premier on note $\nu_p(n)$ la valuation p-adique de n.

Lemme 1. Fixons $k \geqslant 2$ et $w \geqslant 2$ deux entiers. Si $u, v \in \mathbb{N}^* \setminus \{1\}$ sont premiers entre eux et vérifient $uv = w^k$ alors il existe $u', v' \in \mathbb{N}$ tels que $u = (u')^k$ et $v = (v')^k$.

Démonstration. Soient p un facteur premier de u et q un facteur premier de v. Comme u et v sont premiers entre eux on a $p \neq q$. Et puisque $uv = w^k$ on en déduit que $\nu_p(u) = k\nu_p(w)$ et $\nu_q(v) = k\nu_q(w)$. Ainsi on a

$$u = \prod_{p|u} p^{\nu_p(u)} = \left(\prod_{p|u} p^{\nu_p(w)} \right)^k \qquad \text{et} \qquad v = \prod_{q|v} q^{\nu_q(v)} = \left(\prod_{q|v} q^{\nu_q(w)} \right)^k ,$$

ce qui conclut. □

Référence : [FGN, Chap. 3, Exercice 3.35 (Lemme)].

2. Développement

On appelle *nombre de Sophie Germain* tout nombre premier *impair* p tel que $2p + 1$ est encore un nombre premier. Par exemple, $3, 5, 11, ...$ sont des nombres de Sophie Germain.

Théorème 2 (Germain)**.** Soit p un nombre de Sophie Germain. L'équation diophantienne

$$X^p + Y^p + Z^p = 0,$$

n'admet aucune solution $(x, y, z) \in \mathbb{Z}^3$ telle que $xyz \not\equiv 0 \mod p$.

Démonstration. Par l'absurde, supposons qu'il existe une solution $(x, y, z) \in \mathbb{Z}^3$ telle que $xyz \not\equiv 0 \mod p$. Quitte à remplacer (x, y, z) par $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ où $d = \text{pgcd}(x, y, z)$, on peut supposer x, y, z premiers entre eux dans leur ensemble.

Les entiers x, y, z sont deux-à-deux premiers entre eux. En effet, soit par exemple r un facteur premier commun à x et y. Comme $x^p + y^p + z^p = 0$ alors r divise z^p et donc r divise z par le lemme d'Euclide. Absurde.

Comme p est impair, l'équation $x^p + y^p + z^p = 0$ se réécrit $x^p - (-y^p) = (-z)^p$ ou encore

$$(x + y)N = (-z)^p,$$

Date: Année 2024.

avec $N = \sum_{k=0}^{p-1}(-1)^k x^k y^{p-k-1}$. L'entier N est bien premier à $x+y$. En effet, si r est un facteur premier commun à N et $x+y$ alors r^2 divise z^p et donc r divise z (lemme d'Euclide). On a donc

$$0 \equiv N \equiv py^{p-1} \mod r.$$

Par le lemme d'Euclide, soit r divise p c'est-à-dire $r = p$ et donc $xyz \equiv 0 \mod p$, absurde ; soit r divise y et donc r est un facteur premier commun à y et z, absurde.

On peut alors appliquer le lemme 1 : il existe deux entiers $a \in \mathbb{Z}$ tels que

$$x + y = a^p \qquad \text{et} \qquad N = \alpha^p.$$

Avec un raisonnement analogue, il existe aussi $b, c \in \mathbb{Z}$ tels que $y + z = b^p$ et $x + z = c^p$. Comme p est un nombre de Sophie Germain, le nombre $q = 2p + 1$ est encore premier. Supposons que q ne divise ni x, ni y, ni z. Par le petit théorème de Fermat, on a par exemple $(x^p)^2 = x^{q-1} = 1 \mod q$ et donc x^p est une racine du polynôme $X^2 - 1$ dans le corps $\mathbb{Z}/q\mathbb{Z}$. On a donc $x^p = \pm 1 \mod q$. De manière analogue on a $y^p = \pm 1 \mod q$ et $z^p = \pm 1 \mod q$ si bien que

$$0 = x^p + y^p + z^p = \pm 1, \pm 3 \mod q.$$

Or on a $q > 3$. Absurde. Ainsi q divise au moins un des trois entiers x, y, z. Et puisque x, y, z sont premiers entre eux dans leur ensemble, q ne divise qu'un seul de ces trois entiers, disons z.[1] En particulier on a

$$(x+z)+(y+z)-(x+y) = c^p + b^p - a^p = 2z \equiv 0 \mod q \qquad \text{et} \qquad y \equiv b^p \mod q.$$

Comme q ne divise pas y alors q ne divise pas b et donc $y = \pm 1 \mod q$. De manière analogue on a $x \equiv \pm 1 \mod q$ et donc $x + y = a^p \equiv \pm 2, 0 \mod q$. On ne peut pas avoir $a^p \equiv \pm 2 \mod q$ (par petit théorème de Fermat). On a donc $x + y \equiv 0 \mod q$, ce qui implique $\alpha^p = N \equiv \pm py^{p-1} \mod q \equiv \pm p \mod q$ alors que $\alpha^p \equiv 0, \pm 1 \mod q$ (par petit théorème de Fermat) : ABSURDE. □

Référence : [FGN, Chap. 3, Exercice 3.61].

Remarque 3. L'équation $X^p + Y^p + Z^p = 0$ possède une infinité de solutions $(x, y, z) \in \mathbb{Z}^3$ tels que $xyz \equiv 0 \mod p$. Par exemple, $(0, 0, 0), (p, -p, 0), (2p, -2p, 0)$,... Au passage, il n'est pas besoin de supposer p de Sophie Germain pour avoir l'existence de telles solutions (ni même p premier). La condition $xyz \not\equiv 0 \mod p$ est donc une condition de "non trivialité".

3. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) Pourquoi ne peut-on pas avoir $a^p \equiv \pm 2 \mod q$?

(2)

(3)

Références

[FGN] S. Francinou, H. Gianella, et S. Nicolas, *Oraux X-ENS*, Vol. 1, Cassini, 2019.

1. Cette affirmation "arbitraire" découle du fait qu'au début de la preuve nous avons travailler préférentiellement avec $x + y$ (et donc aussi avec N qui interviendra plus tard). Dans le cas où q divise x ou y, il faudrait travailler plutôt avec $x + z$ ou $y + z$ mais ceci n'invalide en rien le raisonnement mené ici.