# 1 Théorème de Sophie Germain

Recasages: 120, 121, 122, 142

**Définition 1.1** (Nombre premier de Sophie Germain)**.** Un nombre premier de Sophie Germain est un nombre premier impair $p$ tel que le nombre $q := 2p + 1$ soit lui aussi premier.

**Théorème 1.1** (Sophie Germain)**.** *Soit $p$ un nombre premier de Sophie Germain. Alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 \pmod p$ et $x^p + y^p + z^p = 0$.*

*Proof.* On va effectuer des raisonnements par l'absurde pendant essentiellement toute la preuve, dont le schéma est grosso-modo le suivant:

- On se ramène à un triplet d'entiers $(x, y, z)$ premiers entre eux deux-à-deux,
- On écrit les sommes $x + y$, $x + z$ et $y + z$ comme des puissances $p$-ièmes,
- On montre qu'alors $q$ divise un entier du triplet, par exemple $x$,
- En travaillant modulo $q$, on aboutit à une contradiction sur la valeur de $p$.

Raisonnons donc par l'absurde et considérons $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 \pmod p$ et $x^p + y^p + z^p = 0$. En divisant tous les éléments du triplet par $pgcd(x, y, z)$, on obtient un nouveau triplet $(x', y', z')$ vérifiant les mêmes hypothèses. Sans perte de généralité, on peut donc supposer $pgcd(x, y, z) = 1$. En fait on a même mieux, puisque nos entiers sont alors nécessairement premiers entre eux. En effet, si (par l'absurde) $pgcd(x, y) > 1$, alors en considérant $p_0$ un diviseur premier de $x$ et $y$, on aurait $p_0 | x^p + y^p = -z^p$, donc $p_0$ divise $z^p$ et alors, par le lemme d'Euclide, $p_0$ divise $z$, ce qui contredit le fait que $x, y$ et $z$ sont premiers entre eux. De la même façon, on a $pgcd(x, z) = pgcd(y, z) = 1$.

On cherche maintenant à écrire $y + z$ comme $a^p$ pour un certain entier $a$. Tout d'abord on a

$$(y + z) \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = y^p + z^p, \tag{1}$$

(formule usuelle pour la somme de deux puissances impaires, se retrouve facilement de la formule peut-être plus connue de la différence:

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

en remplaçant $b$ par $-b$).

On va montrer par l'absurde que $y + z$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux. Par l'absurde donc, soit $p'$ un diviseur premier commun à ces deux

quantités. On a alors $p'|y^p + z^p = -x^p = (-x)^p$ car $p$ est impair, et donc $p'$ divise $x$ par le lemme d'Euclide encore une fois. D'autre part, comme $y \equiv -z \pmod{p}$, on a

$$\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv \sum_{k=0}^{p-1}(-z)^{p-1} \equiv pz^{p-1} \pmod{p'},$$

et donc $p'$ divise $pz^{p-1}$. D'après le lemme de Gauss, deux cas de figures se profilent:

Ou bien $p'$ divise $p$, c'est-à-dire que $p' = p$, et donc que $p$ divise $x$, ce qui contredit les hypothèses sur le triplet, ou bien $p'$ divise $z^{p-1}$, et alors (toujours par le lemme d'Euclide) $p'$ divise $z$. Comme il divise aussi $x$ et que $x$ et $z$ sont premiers entre eux, on aboutit à une contradiction.

Ainsi les quantités $y + z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premières entre elles, et on en déduit par l'égalité (1) l'existence d'entiers $\alpha$ et $a$ tels que $y + z = a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$. (Pour montrer proprement ce qu'on vient de dire, à savoir que si le produit de deux entiers premiers entre eux est une puissance $k$-ième, alors ces deux entiers sont aussi des puissances $k$-ièmes, on écrit les décompositions des deux entiers en produits de premiers.) Un raisonnement identique en tous points montre qu'on peut également considérer des entiers $b$ et $c$ tels que l'on ait $x + z = b^p$ et $x + y = c^p$.

On cherche maintenant à montrer que $q$ divise un entier du triplet, ce qui sera notre point de départ pour la dernière partie de la preuve où l'on travaillera modulo $q$ (ou dans $\mathbb{Z}/q\mathbb{Z}$ si la leçon suggère plutôt ce vocabulaire). On va encore une fois raisonner par l'absurde: supposons que $q$ ne divise ni $x$, ni $y$, ni $z$. Dans ce cas, on commence par montrer que $x^p$, $y^p$ et $z^p$ sont respectivement congrus à $\pm 1 \pmod{q}$ :

Soit $m \in \mathbb{Z}$ tel que $q$ ne divise pas $m$. L'entier $q$ étant premier, on a par le petit théorème de Fermat (ou de manière strictement identique par le fait que $(\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ et en utilisant le théorème de Lagrange):

$$m^{q-1} = m^{2p} \equiv 1 \pmod{q},$$

et donc on a par le fait que, $\mathbb{Z}/q\mathbb{Z}$ étant un corps (puisque $q$ est premier), le polynôme $X^2 - 1$ y admette exactement 2 racines :

$$m^p = \pm 1 \pmod{q}.$$

Ainsi, on a $x^p + y^p + z^p \equiv -3, -1, 1$ ou $3 \pmod{q}$, et donc nécessairement $x^p + y^p + z^p \neq 0$ puisque $q \geq 5$, ce qui contredit les hypothèses sur le triplet. On peut donc supposer que $q$ divise $x$, et dans ce cas $q$ ne divise ni $y$ ni $z$ puisque $pgcd(x, y) = pgcd(x, z) = 1$.

On a toutes les clés en main pour conclure. Commençons par montrer que $q$ divise $a$ en partant du fait que $x$ est un mutliple de $q$. Utilisant cela, on a tout d'abord $b^p + c^p - a^p = 2x \equiv 0 \pmod{q}$ et $y \equiv c^p \pmod{q}$. Or $q$ ne divise pas $y$, donc $q$ ne divise pas $c^p$ et a fortiori ne divise pas $c$, d'où $y \equiv \pm 1 \pmod{q}$ par un raisonnement mené précédemment. De même, $z \equiv \pm 1 \pmod{q}$.

Maintenant, si $q$ ne divise pas $a$ alors $a \equiv \pm 1 \pmod{q}$ et

$$b^p + c^p - a^p \equiv y + z - a^p \equiv -3, -1, 1, 3 \pmod{q},$$

ce qui est absurde puisque $q$ divise $b^p + c^p - a^p$. Donc $q$ divise $a$.

Enfin, comme $y \equiv -z \pmod{q}$, on a

$$\alpha^p = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv \sum_{k=0}^{p-1} y^{p-1} = p y^{p-1} \pmod{q}.$$

Comme $y \equiv \pm 1 \pmod{q}$ et que $p-1$ est impair, il vient $\alpha^p \equiv p \pmod{q}$. Mais on a montré précédemment qu'une puissance $p$-ième ne pouvait être congrue qu'à $-1, 0$ ou $1$ modulo $q$, ce qui est impossible par définition de $q := 2p + 1$.

Conclusion: il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 \pmod{p}$ et $x^p + y^p + z^p = 0$.

□