# Théorème de Germain

## 1 Énoncé

**Théorème :** Soit $x, y, z \in \mathbb{Z}$ et $p$ un nombre premier impair tel que $q = 2p + 1$ est aussi un nombre premier (on dit que $p$ est un nombre premier de Germain, ou de Sophie Germain). Si $x^p + y^p + z^p = 0$, alors $p \mid xyz$, i.e. $p$ divise $x, y$ ou $z$.

## 2 Contexte

Ce théorème a été établi par Sophie Germain dans le cadre de ses recherches sur ce qui était alors la conjecture de Fermat. Elle avait un "grand plan" pour démontrer le théorème, dont on a malheureusement montré bien plus tard qu'il était voué à l'échec. Je vous conseille de visiter la page Wikipédia pour en savoir plus et avoir un peu de contexte historico-mathématique. Il est aussi bon de savoir quelques trucs sur les nombres premiers de Germain, donner quelques exemples ($3, 5$ mais pas $7$), savoir qu'on ne sait pas s'il y en a une infinité.

## 3 La preuve

On suppose par l'absurde l'existence d'entiers vérifiant l'hypothèse mais pas la conclusion.

La preuve se découpe en trois temps. Il me semble important d'avoir compris que le premier temps c'est quelque chose de presque systématique dans des équations diophantiennes (du moins polynomiales) ; le deuxième temps utilise la forme spécifique de l'équation mais fonctionne pour tous les nombres premiers (et même tous les nombres entiers) ; et le troisième temps ne fonctionne que pour les nombres premiers de Germain.

### 3.1 Banalités sur les équations diophantiennes

Les versions sur agreg-maths sautent souvent ce passage, mais il est important pour sa valeur pédagogique, surtout si vous insistez sur ce que j'ai dit au paragraphe précédent. En plus il est indispensable si vous recasez ce développement

dans la 142 (PGCD et PPCM).

L'objectif est de se ramener au cas où $x, y, z$ sont premiers entre eux deux-à-deux. On commence par montrer que si une solution $x, y, z$ existe, il existe une solution *primitive*, i.e. une solution $x', y', z'$ vérifiant $\text{pgcd}(x', y', z') = 1$. Posons $d = \text{pgcd}(x, y, z)$, on définit $x', y', z'$ comme les entiers vérifiant $x = dx', y = dy', z = dz'$. C'est la solution primitive recherchée (on peut détailler au tableau). On suppose donc que la solution $x, y, z$ est primitive.

On va maintenant montrer que $\text{pgcd}(x, y) = 1$. Supposons par l'absurde qu'il existe un nombre **premier** $p'$ (attention à ne pas l'appeler $q$, qu'on réserve pour le nombre $2p + 1$) tel que $p' \mid x$ et $p' \mid y$. On a alors $p' \mid -x^p - y^p = z^p$, donc d'après le lemme d'Euclide $p' \mid z$. Ce qui contredit que la solution est primitive.

## 3.2 Manipulations sur l'équation de Fermat

Écrivons $(-z)^p = x^p + y^p = (x + y) \sum_{k=0}^{p-1} x^k (-y)^{p-1-k}$. Appelons $A$ la somme. Montrons que $A$ et $x + y$ sont premiers entre eux.

Soit $p'$ un nombre premier divisant $A$ et $x + y$. On a alors $x \equiv -y \pmod{p'}$. Modulo $p'$, on a alors $A \equiv \sum_{k=0}^{p-1} x^k x^{p-1-k}$ donc $0 \equiv A \equiv p x^{p-1}$. Grâce à nouveau au lemme d'Euclide, on a $p' \mid p$, i.e. $p' = p$, ou $p' \mid x$. Le premier cas est impossible car on aurait alors $p \mid A \mid z^p$ donc $p \mid z$ ce qui est exclu (attention avec cet argument qui demande de prendre du recul sur l'équation, même le jour J je n'ai pas réussi à le retrouver tout de suite, j'ai dû commencer par le deuxième pour que ça me revienne). Le deuxième cas est aussi impossible car alors $p' \mid x + y - x = y$, ce qui contredit que $x, y$ sont premiers entre eux.

Maintenant qu'on sait que $A$ et $x + y$ sont premiers entre eux et que leur produit est une puissance $p$-ième, on sait que chacun d'eux l'est. On écrit alors $A = \alpha^p$, $x + y = a^p$. On écrit de même $y + z = b^p$, $x + z = c^p$

## 3.3 Considérations modulo $q$ et conclusion

On va maintenant enfin utiliser notre hypothèse sur $p$, en travaillant modulo $q$. En effet, on a trouvé beaucoup de puissances $p$-ièmes, donc on va utiliser le lemme suivant :

**Lemme :** Soit $m$ un entier non divisible par $q$. Alors $m^p \equiv \pm 1 \pmod{q}$.
**Preuve :** D'après le petit théorème de Fermat, on a $(m^p)^2 = m^{2p} = m^{q-1} \equiv 1 \pmod{q}$. Grâce à l'intégrité de $\mathbb{F}_p$, on en déduit le lemme. Il faut savoir détailler : on utilise que 1 et $-1$ sont les seules racines de $X^2 - 1$ dans un anneau intègre.

Le jeu est maintenant d'utiliser ce lemme pour obtenir plein de congruences modulo $q$ qui nous fourniront une contradiction.

On voit d'abord que $q$ divise $x, y$ ou $z$. En effet, dans le cas contraire, $0 = x^p + y^p + z^p \equiv \pm 1$ ou $\pm 3 \pmod{q}$

# 4 Remarques et conseils de présentation

# 5 Questions possibles du jury