12 novembre 2021

Démonstration

Théorème — **de Sophie Germain**

Soit p un nombre impair et un nombre premier de Sophie Germain, c'est à dire tel que $q = 2p+1$ soit premier, alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0\ [p]$ et $x^p + y^p + z^p = 0$.

Les exercices suivants ont pour objectif de nous aider à démontrer le théorème de Sophie Germain.

Cadre : Soit $\mathcal{P}$ l'ensemble des nombres premiers. Considérons p un nombre premier de Sophie Germain impair et $q = 2p + 1$.

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

Exercice n° 1 — Mise en jambes

Pourquoi peut-on supposer que x, y et z sont premiers entre eux dans leur ensemble ?

Dans la suite, nous supposerons que x, y et z sont premiers entre eux dans leur ensemble.

Exercice n° 2

Montrer que x, y et z sont deux à deux premiers entre eux.

Exercice n° 3 — **Lemme**

Soient $u,\ v \in \mathbb{Z}$ avec $u \wedge v = 1$. Démontrer que s'il existe $w \in \mathbb{Z}$ tel que $uv = w^k$, $k \in \mathbb{Z}$ et $k \geq 2$, alors u et v sont des puissances $k^{\text{ième}}$.

Exercice n° 4

Montrer que $y + z$ et $\sum\limits_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux.

Indication :

On pourra remarquer que $(y + z)\left(\sum\limits_{k=0}^{p-1} (-z)^{p-1-k} y^k\right) = y^p + z^p$.

Exercice n° 5 — Facile

Montrer qu'il existe $(a, \alpha) \in \mathbb{Z}^2$ tel que $y + z = a^p$ et $\sum\limits_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p$.

De même on peut montrer qu'il existe $(b, c) \in \mathbb{Z}^2$ tel que $x + z = b^p$ et $x + y = c^p$.

M.Drillet

Exercice n° 6 ★☆

Montrer qu'un des trois nombres x, y ou z est divisible par q.

Dans la suite, considérons que $q|x$.

Exercice n° 7 **Conclusion** ★ ★

1. Calculer $b^p + c^p - a^p$ modulo q.
2. Montrer que $y \equiv \pm 1\ [q]$.
3. En déduire la valeur de a^p modulo q.
4. Conclure.

Référence historique :

En 2001, le plus grand nombre de Sophie Germain connu était $109\,433\,307 \times 2^{66\,452} - 1$, *composé de* $20\,013$ *chiffres. On conjecture qu'il en existe une infinité. Le théorème de Sophie Germain, démontré en 1823 est une résolution partielle du grand théorème de Fermat.*

Référence : X-ENS Algèbre tome 1 de S. FRANCINOU, H. GIANELLA et S. NICOLAS

Dans l'exercice 2, nous pourrons utiliser :

Lemme d'Euclide

Soient b et c deux entiers. Si un nombre premier p divise le produit bc, alors p divise b ou c.

Dans l'exercice 4, nous pourrons utiliser :

Lemme de Gauss

Soient a, b et c trois entiers. Si a divise le produit bc et si a est premier avec b, alors a divise c.

Dans l'exercice 6, nous pourrons utiliser le petit théorème de Fermat :

Proposition :

Si p est un nombre premier et si a est un entier non multiple de p, alors

$$a^{p-1} \equiv 1\ [p].$$

M.Drillet