Développement : Théorème de Sophie Germain

Théorème : p est un nombre premier impair dit de Sophie Germain, ie tel que $q = 2p+1$ est également premier. Alors, il n'existe pas de solution sur $\mathbb{Z}$ à l'équation $x^p+y^p+z^p = 0$ telle que $xyz \not\equiv 0(p)$

1. Historique. — *Une des toutes premières mathématiciennes de l'histoire, elle doit étudier en cachette puis sous un faux nom. Reconnue et appuyé par Lagrange et Gauss. Son théorème faisait partie d'un plan d'attaque du Grand Théorème de Fermat.*

2. Première étape : les sommes deux à deux sont des puissances de p. —

- Rem : $p > 2$ et $q > 5$
- En simplifiant par le pgcd de x, y et z, on se ramène au seul cas où $x \wedge y \wedge z = 1$.
- Nous pouvons en fait remarquer que x, y et z sont deux à deux premiers entre eux. En effet, si x et y avaient un diviseur commun, il devrait aussi diviser z, ce qui contredit le point précédent.
- On raisonne par l'absurde en imaginant un triplet (x, y, z) solution.
- $-x^p = y^p + z^p = (y+z)\Sigma_{k=0}^{p-1} y^k(-z)^{p-1-k} = (y+z)u$
- On remarque alors que $u \wedge (y+z) = 1$ car autrement :
  - si $\exists p_0 \in P$ divise u et $(y+z)$ nous avons :
  - p_0 divise x^p et donc x.
  - En passant au module $\Sigma_{k=0}^{p-1} y^k(-z)^{p-1-k} \equiv \Sigma_{k=0}^{p-1} y^{p-1} = py^{p-1} \equiv u \equiv 0$ modulo p_0.
  - Et donc, comme $x \wedge y = 1$, p divise p_0 et donc $p = p_0$
  - Donc p divise x et $xyz \equiv 0(p)$ ce qui est contraire aux hypothèses.
- Comme le produit de u et $(y+z)$ est une puissance de p et que ces deux termes sont premiers entre eux, chacun des deux est lui-même une puissance de p.
- $\exists a, \alpha \in \mathbb{Z}$ tels que $(y+z) = a^p; u = \alpha^p; x^p = a^p \times \alpha^p$.
- Par symétrie, $\exists a, b, c \in \mathbb{Z}$ tels que $(x+y) = c^p; (y+z) = a^p; (x+z) = b^p$

3. Deuxième étape : q divise x. —

- Lemme : Si m n'est pas divisible par q alors $m^p \equiv \pm 1(q)$
  - D'après le petit théorème de Fermat $m^{q-1} \equiv 1(q)$ ie $(m^p)^2 \equiv 1(q)$.
  - Or, q étant premier, $\mathbb{Z}/q\mathbb{Z}$ est un corps et on a donc $m^p \equiv \pm 1(q)$.
- q divise un des trois x, y ou z. En effet, si aucun ne l'était, en vertu du lemme précédent, appliqué à m valant tour à tour x, y ou z nous aurions :
- $x^p+y^p+z^p \equiv$ à $1+1+1 = 3$ ou $1-1-1 = -1$ ou $-1-1-1 = -3$ ou $-1+1+1 = 1$ modulo q.
- Or, $x^p + y^p + z^p$ vaut 0 par hypothèse et $q > 3$ donc q divise au moins un des x, y, z.
- Comme les trois nombres sont premiers entre eux, il n'en divise qu'un seul. On supposera qu'il s'agit de x.

4. Troisième étape : q divise y+z. —

- q divise x et donc $2x = (x+y)+(x+z)-(y+z) = -a^p + b^p + c^p \equiv 0(q)$
- puisque $x \equiv 0(q)$, $y \equiv c^p(q)$ et aussi, d'après le lemme, $y \equiv \pm 1(q)$.
- de manière symétrique, $z \equiv \pm 1(q)$.
- On a donc $-a^p + b^p + c^p \equiv -a^p \pm 1 \pm 1 \equiv 0(q)$ ie $a^p(q) \in \{0, 2, -2\}$
- D'après la contraposée du lemme, a est divisible par q
- Donc $y + z \equiv 0(q)$.

5. Quatrième étape : retour sur u et contradiction. —

- Puisque $y \equiv -z(q)$, si on reprend l'expression de u et on passe aux restes modulo q, on a :
- $[u = \alpha^p = \Sigma_{k=0}^{p-1} y^k(-z)^{p-1-k}] \equiv [\Sigma_{k=0}^{p-1} y^{p-1} = py^{p-1}]$
- Or, $y \equiv \pm 1(q)$ et $p-1$ est pair. Donc $\alpha^p \equiv p(q)$
- Or, d'après le lemme cela est impossible. *Contradiction.*

.

Sources :Francinou et Gianella - tome 1

December 11, 2017

Bruno Nitrosso, EPP et candidat libre