Prérequis. Petit théorème de Fermat.

Théorème 0.0.1. *Soit p un nombre premier impair tel que $q = 2p + 1$ le soit aussi. Alors il n'existe aucune solution $(x, y, z) \in \mathbf{Z}^3$ à l'équation $x^p + y^p + z^p = 0$ avec $xyz \not\equiv 0$ modulo p.*

Démonstration. Par l'absurde, soit (x, y, z) une telle solution.

Montrons que l'on peut supposer les entiers premiers entre eux deux à deux. Si d est le pgcd de x, y et z alors $(x/d, y/d, z/d)$ est encore une solution, donc on peut supposer $d = 1$. Ensuite si un premier p_0 divise x et y alors il divise $x^p + y^p$ donc aussi z^p donc z, d'où p_0 divise d. Donc on peut supposer x et y premier entre eux, de même pour les deux autres paires.

Montrons que $y+z$ est une puissance p-ème. Soit p_0 un diviseur premier commun de $y + z$ et de :

$$\beta = \sum_{k=0}^{p-1} (-z)^{p-k-1} y^k.$$

Alors :

$$\begin{aligned}(y + z)\beta &= \sum_{k=0}^{p-1} \left((-z)^{p-k-1} y^{k+1} - (-z)^{p-k} y^k \right) \\ &= y^p + z^p = -x^p = (-x)^p.\end{aligned}$$

Donc p_0^2 divise $y^p + z^p = (-x)^p$, en particulier p_0 divise x. Comme $y \equiv -z$ modulo p_0, on a aussi :

$$0 \equiv \beta \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1} \ [p_0]$$

donc p_0 divise py^{p-1}.

Si p_0 divise p alors $p_0 = p$ donc p divise x, ce qui est supposé faux. Donc p_0 divise y^{p-1} donc y, d'où p_0 divise à la fois x, y et z : c'est absurde.

Conclusion : $y+z$ et β doivent être premiers entre eux. Comme leur produit $(-x)^p$ est une puissance p-ème, ce sont eux-mêmes des puissances p-èmes. Le même raisonnement marche pour les autres sommes, et l'on écrit alors :

$$\begin{aligned}\beta &= \alpha^p, \\ y + z &= a^p, \\ x + z &= b^p, \\ x + y &= c^p.\end{aligned}$$

Montrons que l'un des trois nombres x, y ou z est multiple de q. Soit $m \in \mathbf{Z}$ non multiple de q. Par le petit théorème de Fermat, $m^{q-1} \equiv (m^p)^2 \equiv 1$ modulo q donc $m^p \equiv \pm 1$.

Si q ne divisait ni x, ni y, ni z, on aurait alors cette congruence pour $m = x$, y et z. En sommant, aucun cas n'amène à 0 modulo q car $q \geqslant 5$. Sans perdre de généralité, disons que c'est x qui est multiple de q.

Conclusion. On a :

$$c^p + b^p - a^p = 2x \equiv 0 \ [q]$$

et $y \equiv x + y \equiv c^p \ [q]$. Comme q ne peut pas diviser y, on a comme au paragraphe précédent $y \equiv c^p \equiv \pm 1$ modulo q. De même, $z \equiv \pm 1$.

Si q ne divisait pas a alors on aurait $a^p \equiv \pm 1$ et la somme $c^p + b^p - a^p$ ne pourrait pas valoir 0 modulo q. Donc q divise a, d'où $y + z \equiv a^p \equiv 0$ modulo q donc :

$$\beta \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1} \equiv p(\pm 1)^{p-1} \equiv p \ [q]$$

ce qui est absurde car $\beta = \alpha^p$ est congru soit à 0 soit à ± 1 modulo q, et certainement pas à p. □

Remarques.

- La démonstration est assez longue et technique à mémoriser. Mais en la découpant en étapes, on s'en sort mieux.
- Il faut savoir démontrer le petit théorème de Fermat : si p est un nombre premier et a n'est pas multiple de p, alors a^{p-1} est congru à 1 modulo p. Pour le démontrer, a est dans le groupe multiplicatif du corps $\mathbf{Z}/p\mathbf{Z}$, groupe qui est d'ordre $p - 1$.
- C'est dommage de faire ce développement sans connaître un peu le grand théorème de Fermat. Il a été énoncé au début du dix-septième siècle, démontré par Wiles (avec l'aide de Frey, Serre, Ribet, Hellegouarch, Shimura, Taniyama, ...) en 1994, et entre-temps attaqué par à peu près tout le monde, dont Sophie Germain qui a démontré son théorème en 1823 (donc à mi-chemin, 200 ans après l'énoncé et 170 ans avant la démonstration complète). Le théorème de Sophie Germain est évidemment un cas particulier du dernier théorème de Fermat.
- Un nombre premier p tel que $q = 2p + 1$ soit aussi premier est appelé *nombre premier de Sophie Germain*. L'existence d'une infinité de tels nombres est encore une conjecture (A005384 sur l'OEIS). Les nombres premiers de Sophie Germain peuvent être utilisés en cryptographie parce que $(\mathbf{Z}/(2p+1)\mathbf{Z})^\times$ a un sous-groupe d'ordre premier très grand.

Recasages.

- 120 : On utilise à fond l'arithmétique modulaire, et le petit théorème de Fermat qui est vraiment un théorème à propos de l'anneau $\mathbf{Z}/q\mathbf{Z}$. Le théorème de Sophie Germain est vraiment une application de l'étude de ces anneaux.

— 121 : On utilise plein de propriétés des nombres premiers, et on démontre un cas particulier du dernier théorème de Fermat, avec des liens forts avec la primalité.
— 126 : Rien à ajouter, tout est dans le titre de la leçon. C'est probablement l'équation diophantienne la plus renommée.
— 142 : Un peu limite. L'argument utilisé au début pour dire que les nombres peuvent être supposés premiers entre eux est souvent pratique, mais il n'est pas au centre du développement.