Sophie Germain (1776 – 1831)

Forme édulcorée du Théorème de Sophie Germain
Soit p un nombre premier de Sophie Germain, c'est-à-dire impair et tel que $q = 2p + 1$ soit premier. Alors il n'existe pas de solution $(x, y, z) \in \boldsymbol{Z}^3$ de l'équation
$x^p + y^p + z^p = 0$ *telle que* $xyz \neq 0 \text{ mod. } p$

Je n'ai jamais pu arriver à l'infini, quoique j'aie reculé bien loin les limites par une méthode de tâtonnement trop longue pour qu'il me soit possible de l'exposer ici. Je n'oserais même pas affirmer qu'il n'existe pas une limite au-delà de laquelle tous les nombres de la forme $2Np + 1$auraient deux résidus p-ièmes placés de suite dans la série des nombres naturels. C'est le cas qui intéresse l'équation de Fermat.

Vous concevrez aisément, Monsieur, que j'ai dû parvenir à prouver que cette équation ne serait possible qu'en nombres dont la grandeur effraie l'imagination. Car elle est encore assujettie à bien d'autres conditions que je n'ai pas le temps d'énumérer à cause des détails nécessaires pour en établir la véracité. Mais tout cela n'est encore rien, car il faut l'infini et non pas le très grand.

En effet, rien ne pourrait me prouver d'une manière plus flatteuse et moins équivoque, que les attraits de cette science, qui ont embelli ma vie de tant de jouissances, ne sont pas chimériques, que la prédilection, dont vous l'avez honorée.