Sophie Germain et le théorème de Fermat

Catherine Goldstein
CNRS-Institut de mathématiques de Jussieu-Paris Rive gauche

1 Une mathématicienne

Sophie Germain (1776–1831) s'est passionnée dès l'adolescence pour les mathématiques, en particulier la théorie des nombres et l'analyse. Autodidacte, ne pouvant être élève de la toute nouvelle École polytechnique qui était alors réservée aux hommes, elle a toutefois réussi à s'en procurer les cours, accédant ainsi à la formation la plus avancée de son époque en mathématiques. Elle a eu des échanges scientifiques, parfois entamés sous un nom d'emprunt masculin, avec des mathématiciens importants, Adrien-Marie Legendre, Joseph-Louis Lagrange, Carl Friedrich Gauss, Joseph Fourier, etc. En 1816, elle a reçu un prix de l'Académie des sciences pour ses travaux sur la vibration des surfaces élastiques. Ses réflexions philosophiques ont été publiées de manière posthume.

2 Gauss et les congruences

Mais ses principaux résultats concernent la théorie des nombres. Elle fait partie des rares personnes à avoir étudié en détail dès leur parution les célèbres *Disquisitiones arithmeticae* ("Recherches arithmétiques" en français) de Gauss, un traité difficile qui introduit de nombreuses notions nouvelles. Sans savoir encore qu'elle est une femme, Gauss, pourtant rarement enthousiaste sur les travaux des autres, écrit en 1805 à un ami scientifique qu'il a repris ses recherches en théorie des nombres en partie grâce à "plusieurs lettres de LeBlanc [le nom d'emprunt de Sophie Germain] de Paris, qui a étudié mes Disq. Arith. avec une vraie passion, s'y est tout à fait initié et m'a envoyé à leur propos de fort jolies remarques".

Dans son ouvrage, Gauss définit en particulier la notion de congruence :
Deux entiers a et b sont congrus modulo un troisième entier n si n divise la différence $a-b$.
Par exemple, 1 et 27 sont congrus modulo 13, car 13 divise leur différence, $27-1=2\cdot 13$. Cette notion s'avère très utile pour étudier la divisibilité, car on peut ajouter ou multiplier des congruences entre elles comme s'il s'agissait d'égalités. Gauss a d'ailleurs noté cette relation par un signe proche de l'égalité, qu'on utilise toujours : $a \equiv b \bmod n$.

3 Le programme de Sophie Germain

Sophie Germain a eu l'idée de se servir de ces congruences pour aborder le Grand Théorème de Fermat, qui affirme que :
L'équation $x^p+y^p=z^p$ n'a pas de solutions x, y, z en entiers tous non nuls, dès que l'exposant entier p est strictement plus grand que 2.

Cet énoncé de Pierre Fermat, magistrat toulousain et célèbre mathématicien du 17e siècle, n'a été démontré complètement qu'en 1994. Au tout début du 19e siècle, il était prouvé seulement pour $p=3$ et $p=4$; Sophie Germain a été la première à obtenir des résultats de nature plus générale. Pour un exposant p premier, elle espérait construire une infinité de nombres premiers auxiliaires θ de la forme $2Np+1$ (avec N entier) qui, pour toute solution x, y, z de l'équation $x^p+y^p=z^p$, diviseraient nécessairement un des entiers x, y, z. Comme un entier non nul n'est divisible que par un nombre fini de nombres premiers, cela aurait montré que l'équation de Fermat $x^p+y^p=z^p$ n'a pas de solutions non nulles.

3.1 Un théorème

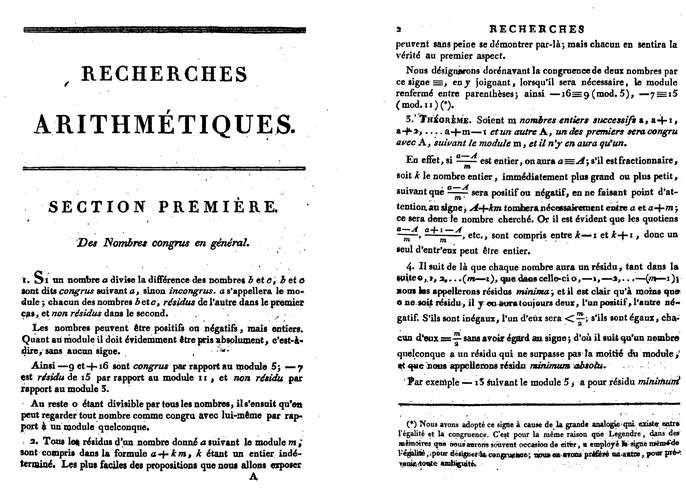
En vue de cette construction, Sophie Germain prouva plusieurs théorèmes intermédiaires, en particulier le suivant :
Si p est un nombre premier impair et s'il existe un nombre premier auxiliaire θ tel que (1) p n'est pas congru à une puissance p-ième modulo θ et (2) il n'existe pas deux puissances p-ièmes consécutives modulo θ [autrement dit, $p \equiv a^p \pmod{\theta}$ et $a^p \equiv 1+b^p \pmod{\theta}$ sont impossibles], alors dans toute solution x, y, z de l'équation de Fermat $x^p+y^p=z^p$, l'un des x, y, z est divisible par θ et l'un des x, y, z est divisible par p^2.
Par exemple, pour $p=3$, on peut choisir comme nombre premier auxiliaire $\theta=13$. Les puissances 3-ièmes modulo 13 sont 1, 5, 8 et 12, les hypothèses du théorème de Germain sont donc vérifiées. On en déduit que si x, y, z vérifiaient $x^3+y^3=z^3$, l'un des nombres x, y, z serait divisible par 13 et l'un des nombres x, y, z serait divisible par 9.

Pour de nombreux p, ce théorème permet déjà de démontrer la moitié du théorème de Fermat, c'est-à-dire qu'il n'y a pas de solutions entières non nulles et premières à p de l'équation $x^p+y^p=z^p$.

3.2 Les nombres premiers de Sophie Germain

Mais comme elle-même l'a découvert assez vite, l'espoir initial de Sophie Germain ne pouvait aboutir ; pour $p=3$, par exemple, il n'y a pas une infinité de premiers auxiliaires valables, seuls 7 et 13 le sont. Cependant les résultats qu'elle avait obtenus et la recherche de couples de nombres premiers $(p, 2Np+1)$ sont intéressants en eux-mêmes. Les nombres premiers p tels que $2p+1$ est aussi un nombre premier sont maintenant appelés des nombres premiers de Sophie Germain en son honneur. Ces nombres interviennent en cryptographie et pour engendrer des nombres pseudo-aléatoires, c'est-à-dire des nombres qui miment le hasard. Mais on ne sait toujours pas s'il en existe ou non une infinité !

FIGURE 1 – Sophie Germain



RECHERCHES

ARITHMÉTIQUES.

SECTION PREMIÈRE.

Des Nombres congrus en général.

1. Si un nombre a divise la différence des nombres b et c, b et c sont dits *congrus* suivant a, sinon *incongrus*. a s'appellera le module ; chacun des nombres b et c, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire, sans aucun signe.

Ainsi -9 et $+16$ sont *congrus* par rapport au module 5 ; -7 est *résidu* de 15 par rapport au module 11, et *non résidu* par rapport au module 5.

Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque.

2. Tous les résidus d'un nombre donné a suivant le module m, sont compris dans la formule $a+km$, k étant un entier indéterminé. Les plus faciles des propositions que nous allons exposer

A

2 RECHERCHES

peuvent sans peine se démontrer par-là ; mais chacun en sentira la vérité au premier aspect.

Nous désignerons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécessaire, le module renfermé entre parenthèses ; ainsi $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$ (*).

3. THÉORÈME. Soient m *nombres entiers successifs* a, $a+1$, $a+2$, ... $a+m-1$ *et un autre* A, *un des premiers sera congru avec* A, *suivant le module* m, *et il n'y en aura qu'un.*

En effet, si $\frac{a-A}{m}$ est entier, on aura $a \equiv A$; s'il est fractionnaire, soit k le nombre entier, immédiatement plus grand ou plus petit, suivant que $\frac{a-A}{m}$ sera positif ou négatif, en ne faisant point d'attention au signe, $A+km$ tombera nécessairement entre a et $a+m$; ce sera donc le nombre cherché. Or il est évident que les quotiens $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, etc., sont compris entre $k-1$ et $k+1$, donc un seul d'entr'eux peut être entier.

4. Il suit de là que chaque nombre aura un résidu, tant dans la suite $0, 1, 2, \ldots (m-1)$, que dans celle-ci $0, -1, -2, \ldots -(m-1)$; nous les appellerons résidus *minima* ; et il est clair qu'à moins que a ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif. S'ils sont inégaux, l'un d'eux sera $< \frac{m}{2}$; s'ils sont égaux, chacun d'eux $= \frac{m}{2}$ sans avoir égard au signe ; d'où il suit qu'un nombre quelconque a un résidu qui ne surpasse pas la moitié du module, et que nous appellerons résidu *minimum absolu*.

Par exemple -15 suivant le module 5, a pour résidu *minimum*

(*) Nous avons adopté ce signe à cause de la grande analogie qui existe entre l'égalité et la congruence. C'est pour la même raison que Legendre, dans des mémoires que nous aurons souvent occasion de citer, a employé le signe même de l'égalité, pour désigner la congruence ; nous en avons préféré un autre, pour prévenir toute ambiguïté.

FIGURE 2 – Les congruences dans les *Recherches arithmétiques* de C.F. Gauss, 1801. Trad. fr. de A.-C.-M. Poullet-Delisle, 1807

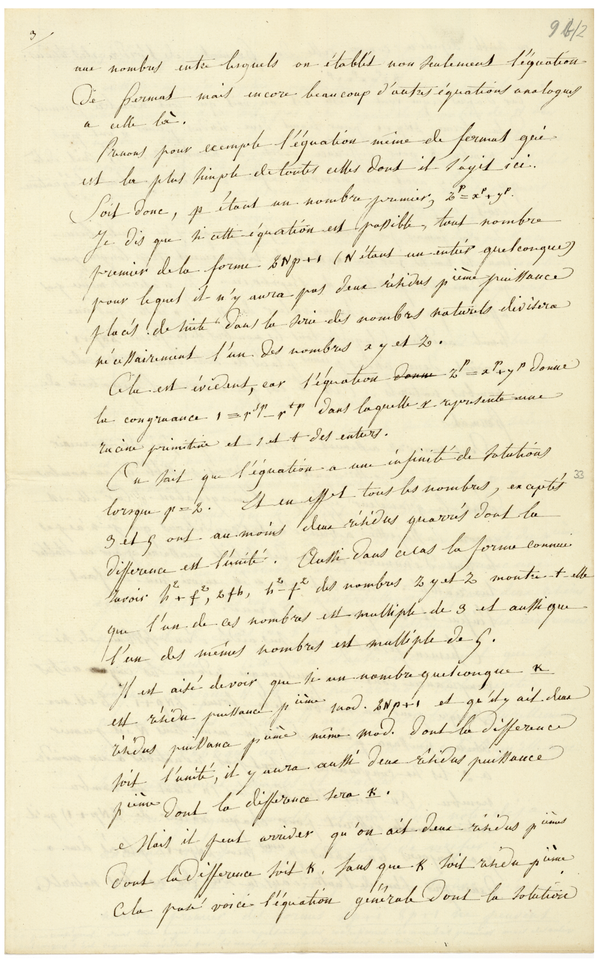


FIGURE 3 – Lettre de Sophie Germain à Gauss sur le théorème de Fermat 12 mai 1819 (extrait). ©SUB Göttingen

4 Références

Andrea Del Centina, Unpublished manuscripts of Sophie Germain and a revaluation of work on Fermat's Last Theorem, *Archive for History of Exact Sciences* **62** (2008), 349–392.
Andrea Del Centina et Alessandra Fiocca, The correspondence between Sophie Germain and Carl Gauss, *Archive for History of Exact Sciences* **66** (2012), 585–700.
Reinhard Laubenbacher et David Pengelley, "Voici ce que j'ai trouvé" : Sophie Germain's grand plan to prove Fermat's Last Theorem, *Historia Mathematica* **37** (2010), 641–692.

IMJ-PRG Institut de Mathématiques de Jussieu-Paris Rive Gauche
INTEGER Institutional Transformation for Effecting Gender Equality in Research