Le théorème de Fermat vu par M. Le Blanc

Ann Kiefer*
akiefer@vub.ac.be

Résumé

Nous présenterons l'idée de Sophie Germain (aussi connue sous le nom de M. Le Blanc) pour attaquer la preuve du théorème de Fermat. Après un bref récapitulatif de la biographie de Sophie Germain, nous analyserons son plan de preuve général et donnerons un aperçu des mathématiques sous-jacentes.

Contents

1 Biographie **52**
2 Rappels mathématiques **54**
3 Le travail de Sophie Germain **56**
4 Les nombres premiers de Sophie Germain **63**
5 Bibliographie **65**

*Ann Kiefer est une doctorante et Aspirant FWO de la Vrije Universiteit Brussel. Elle est titulaire d'un Master en Sciences Mathématiques de l'Université libre de Bruxelles et travaille en théorie des groupes.

Figure 1 — Une rue de Paris porte encore son nom.

1 Biographie

Née en 1779 dans une famille bourgeoise, Sophie Germain s'est intéressée très tôt à l'étude des mathématiques. Or, à cette époque, les femmes n'étaient pas censées faire des études. Elles bénéficiaient certes d'un certain niveau d'éducation, mais dans le simple intérêt de leur transmettre une culture générale afin qu'elles puissent engager des conversations, dans les salons, avec de futurs maris potentiels. Un livre très à la mode à cette époque était le livre *Le Newtonianisme pour les dames*, écrit par l'italien Francesco Algarotti. Le but de ce livre était de rendre des sujets qu'on considérait masculins, comme les sciences, intéressants pour les femmes. On y trouvait ainsi toutes sortes d'explications pour le moins singulières et au contenu mathématique fort douteux, comme par exemple la phrase suivante qui tente d'expliquer la loi de la gravitation en l'inverse du carré de la distance : « *Cette loi d'attraction inverse pourrait s'appliquer à l'amour : après huit jours de séparation l'amour est soixante-quatre fois plus intense*. » Il n'est alors pas difficile de s'imaginer que ce n'est pas un livre pareil qui a éveillé l'intérêt de Sophie Germain pour les mathématiques. En effet, le livre qui a incité Germain à s'intéresser aux mathématiques est un ouvrage de Jean-Étienne Montucla sur l'histoire des mathématiques. Dans cet ouvrage Germain découvrit la curieuse histoire de la mort d'Archimède : un jour Archimède était en train de réfléchir à un problème de géométrie et pour cela il avait dessiné des figures dans le sable. Vint alors un soldat qui lui demanda de se présenter et de s'identifier. Selon la légende, Archimède, concentré sur ses figures, eut pour seule réponse : *« Je ne veux pas être dérangé, et ne piétine pas mes figures sur le sable*. » Le soldat le tua immédiatement d'un coup d'épée. Cette histoire fascinait Germain. Elle se disait que si un homme pouvait être pris par l'étude des mathématiques au point de mourrir pour cela, ce sujet devrait être fascinant et vaudrait sûrement la peine d'être étudié. C'est ce qui poussera Germain vers l'étude des mathématiques. Bien sûr ceci n'était pas du tout bien vu par ses parents et, à cette époque, on disait des mathématiques qu'elles pouvaient « *mener les femmes à la folie, leur cerveau n'étant pas capable de supporter un tel effort*. » Les parents essayaient donc tout pour empêcher Germain d'étudier, allant parfois jusqu'à la priver de vêtements et de bougies pendant la nuit, mais son désir de comprendre cette science était tel qu'elle en vint à devoir voler en secret quelques bougies et quelques draps, de sorte à pouvoir étudier la nuit. Il est dit que les parents finirent par accepter la passion de leur fille.

En 1794 l'École Polytechnique ouvrit ses portes à Paris, mais il était bien sûr hors question qu'une femme atteigne les cours donnés à cet école. Or, Antoine Auguste Le Blanc, un ami de Sophie, y était inscrit comme élève et était d'accord que Germain se procure les cours en utilisant son nom. Un jour, Le Blanc quitta Paris sans avertir l'école et Germain continua ainsi à utiliser son nom pour se procurer les cours et pour participer aux exercices posés aux étudiants. Mais Germain avait du talent et Lagrange, un des meilleurs mathématiciens de son époque, qui était professeur à l'École Polytechnique à ce moment-là, le remarqua et demanda à rencontrer cet étudiant en personne. Sophie Germain, forcée de

révéler sa vraie identité, surprit bien évidemment le professeur qui, loin de le prendre mal, devint ainsi son mentor ! C'est donc avec l'aide de Lagrange qu'elle fit ses premiers pas dans la recherche en mathématiques, s'intéressant très tôt au théorème de Fermat.

C'est en vue d'une démonstration de ce théorème qu'elle commença à développer ses premières idées originales. Or, à ce moment, le plus grand spécialiste en théorie des nombres était Carl Friedrich Gauss et en 1804, à l'âge de 28 ans, Sophie Germain décida de lui écrire pour lui expliquer son idée de démonstration. Par peur de ne pas être prise au sérieux, elle utilisa à nouveau le pseudonyme d'Antoine Auguste Le Blanc. Il se trouve que Gauss, qui n'avait malheureusement pas le temps de tout lire, lut tout de même les parties de ses lettres qui l'intéressèrent le plus et répondit aimablement. Commence alors une riche correspondance entre les deux, à peine quelques années avant l'envoi des troupes Napoléoniennes en Allemagne, événement qui démasquera une fois de plus la mathématicienne, bien que d'une façon bien différente de l'épisode de l'École Polytechnique et qui aura cette fois attrait non pas au talent mais à l'amitié qui s'était installée entre les deux correspondants. Effectivement, ayant peur pour Gauss, Germain demanda à des amis faisant partie des troupes envoyées en Allemagne de protéger son ami allemand. Or, ces derniers informèrent le brillant mathématicien qu'il devait sa protection à une certaine Mademoiselle Germain, que Gauss ne tarda pas à identifier avec son correspondant Antoine Auguste Le Blanc. Si la révélation de l'identité de Germain se déroule ici d'une manière différente, elle trouve pour écho la même réaction : loin d'être rebuté, Gauss eût même une réaction très positive et déclara même dans une lettre que, s'il était déjà fasciné par les travaux de Le Blanc, le savoir réellement une femme ne faisait que l'enthousiasmer davantage ! D'aucuns rétorqueront, avec toutes les raisons du monde, qu'une telle réaction, bien que très progressiste pour l'époque, révèle tout de même à quel point la femme était perçue comme inférieure dans la société de l'époque. Cependant, il n'y a pas qu'en mathématiques que Gauss était en avance sur son temps, puisqu'il dira que ce n'est pas l'infériorité intellectuelle supposée des femmes (chose à laquelle il ne croyait pas) qui exacerbait sa fascination pour les travaux de Germain, mais bien le fait que le genre opposé n'avait accès qu'à une éducation réduite. Leur amitié continua ainsi par correspondance jusqu'à ce que, un peu plus tard, Gauss fusse nommé directeur à l'Observatoire de Göttingen et commence à manquer de plus en plus de temps à consacrer à Germain.

Les résultats de Germain sur le théorème de Fermat ne seront validés qu'en 1830 dans la publication *Théorie des nombres* de Legendre. Dans une note en bas de page, ce dernier explique qu'un des théorèmes du livre est dû à Sophie Germain. Il faut effectivement garder en mémoire que son approximation du théorème de Fermat constitue, entre 1738 et 1840, une des avancées les plus importantes vers sa démonstration (qui ne viendra cependant que bien plus tard).

Le nom de Sophie Germain se trouve ainsi très souvent mentionné en association avec le théorème de Fermat, bien que ses contributions ne s'y soient pas limitées, bien au contraire ! En effet, elle a également fait des contributions à la théorie de l'élasticité des corps, pour lesquelles elle obtint le prix de l'Académie des Sciences. Elle obtint en outre la médaille honorifique de l'Institut de France et fut la première femme ayant le droit d'assister aux séances de l'Académie des Sciences sans être mariée à l'un des scientifiques présents. En 1830 elle se verra même décerner le titre de docteur *honoris causa* à l'université de Göttingen, titre qu'elle n'aura malheureusement jamais eu la chance d'accepter en personne, car c'est en 1831 déjà qu'elle succombera à un cancer du sein.

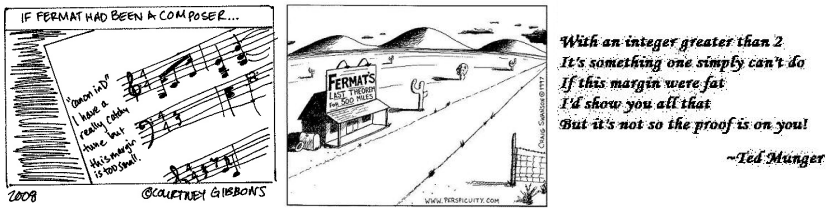

Figure 2 — Le théorème de Fermat est une source d'inspiration.

Pour plus de détails sur Sophie Germain, nous invitons le lecteur à consulter les ouvrages [4] et [6].

2 Rappels mathématiques

2.1 Le grand théorème de Fermat

C'est en 1670 que Pierre de Fermat conjecture le théorème pour la première fois.

Théorème 1. *Pour $n > 2$ l'équation $x^n + y^n = z^n$ n'admet pas de solution en nombres entiers.*

Fermat écrit en fait l'énoncé du théorème (sans la preuve) dans une copie du livre *Arithmetica* de Diophante. Le problème 8 de ce livre traite de comment un carré donné peut être écrit comme somme de deux carrés, autrement dit, si k est un nombre rationnel donné, comment peut-on trouver des rationnels u et v satisfaisant l'équation $k^2 = u^2 + v^2$. La note que Fermat laisse en marge de ce problème est la suivante :

> Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.
>
> On ne peut exprimer un cube comme une somme de deux cubes, un bicarré comme une somme de deux bicarrés, et plus généralement une puissance parfaite comme une somme de deux mêmes puissances. J'en ai découvert une démonstration tout à fait remarquable. Mais ma marge est trop étroite pour la contenir.

Seule la démonstration de Fermat du cas $n = 4$ a été retrouvée. En 1753, Euler a pu démontrer le cas $n = 3$ et en 1825 Dirichlet et Legendre ont traité le cas $n = 5$. En 1839, Lamé a démontré le cas $n = 7$, mais c'est seulement en 1995, plus de trois siècles après l'énoncé du théorème, que Andrew Wiles trouve enfin une démonstration de cette conjecture, en utilisant la théorie des courbes elliptiques. Au temps de Sophie Germain, seuls les cas $n = 4$ et $n = 3$ étaient donc connus. Le fait que des mathématiciens, ainsi que des amateurs, aient cherché pendant plus de trois siècles une démonstration de cette conjecture, combiné à la simplicité de l'énoncé de ce théorème, aura eu comme résultat que le théorème de Fermat est probablement l'un des théorèmes mathématiques les plus connus en dehors du

monde académique. On trouve ainsi sur ce théorème diverses blagues, comme le montre la figure 2 on the preceding page, des poèmes et même des histoires d'amour. Dans le livre *True Tales of American Life* de Paul Auster apparaît une nouvelle, intitulée *Mathematical Aphrodisiac*, écrite par Alex Galt, dans laquelle le théorème de Fermat est évoqué.

2.2 Quelques lemmes et théorèmes nécessaires

Dans cette sous-section, nous allons survoler quelques lemmes et théorèmes connus et facilement démontrables, qui seront nécessaires à la compréhension de la partie principale de ce texte.

Nous commençons par rappeler quelques lemmes en relation avec le théorème de Fermat, déjà connus à l'époque de Sophie Germain.

Lemme 2. *Si l'équation $x^n + y^n = z^n$ n'admet pas de solution en nombres entiers avec x, y et z premiers entre eux, l'équation n'admet pas de solution tout court.*

Démonstration. Supposons que l'équation $x^n + y^n = z^n$ n'admette pas de solution en nombres entiers x, y et z premiers entre eux, mais qu'elle admet une solution X, Y, Z. Alors il existe un nombre entier m tel que $m \mid X, Y, Z$. Prenons m maximal. On a

$$X^n + Y^n = Z^n \Leftrightarrow \left(\frac{X}{m}\right)^n + \left(\frac{Y}{m}\right)^n = \left(\frac{Z}{m}\right)^n$$

et donc $\frac{X}{m}$, $\frac{Y}{m}$ et $\frac{Z}{m}$ sont solutions de l'équation $x^n + y^n = z^n$. Comme m est maximal, les trois nombres entiers sont premiers entre eux, ce qui donne la contradiction souhaitée. □

Lemme 3. *Si $4 \mid n$, l'équation $x^n + y^n = z^n$ n'admet pas de solution en nombres entiers.*

Démonstration. Supposons que $4 \mid n$ et que l'équation $x^n + y^n = z^n$ admette une solution en nombres entiers X, Y et Z. Alors il existe un nombre entier m tel que $n = 4m$ et on a

$$\begin{aligned} & X^n + Y^n = Z^n \\ \Leftrightarrow & X^{4m} + Y^{4m} = Z^{4m} \\ \Leftrightarrow & (X^m)^4 + (Y^m)^4 = (Z^m)^4. \end{aligned}$$

On aurait donc trouvé une solution en nombres entiers à l'équation $x^4 + y^4 = z^4$, ce qui est en contradiction avec la preuve de Fermat comme quoi cette équation n'a pas de solution en nombres entiers. □

Grâce aux lemmes 2 et 3, il suffit de démontrer que l'équation $x^p + y^p = z^p$ n'admet pas de solution en nombres entiers premiers entre eux pour p étant un nombre premier impair afin de démontrer le théorème de Fermat. En effet, supposons que l'équation $x^p + y^p = z^p$ n'admette pas de solutions mais que l'équation $x^n + y^n = z^n$ en admette une pour n non premier. Supposons alors qu'il existe un nombre premier impair p qui divise n, c'est-à-dire $n = pm$. Si X, Y, Z satisfont $X^n + Y^n = Z^n$, alors X^m, Y^m, Z^m sont solutions de l'équation $x^p + y^p = z^p$, ce qui contredit l'hypothèse du départ. Si n n'est pas divisible par un nombre premier impair, alors n est de la forme $n = 2^m$ pour un nombre entier m. Or comme $n > 2$,

n est divisible par 4, ce qui est en contradiction avec le lemme 3. Le lemme 2 implique alors que les solutions x, y, z peuvent être choisies premières entre elles.

Avant de passer au travail de Sophie Germain, rappelons quelques théorèmes connus, qu'on ne démontrera pas ici. Le premier théorème est connu sous le nom de *petit théorème de Fermat*.

Théorème 4 (Le petit théorème de Fermat). *Soient p un nombre premier et $a \in \mathbb{Z}$ avec $p \nmid a$. Alors*

$$a^{p-1} \equiv 1 \mod p.$$

Le deuxième théorème est dû à Euler.

Théorème 5. *Soient $p \neq \theta$ deux nombres premiers. Alors $x^p \equiv a \pmod{\theta}$ admet une solution en x si et seulement si $a^{\frac{\theta-1}{d}} \equiv 1 \pmod{\theta}$ où $d = \operatorname{pgcd}(p, \theta - 1)$.*

3 Le travail de Sophie Germain

Dans cette section nous considérons une partie des travaux de Sophie Germain sur le théorème de Fermat. Une étude plus complète peut être trouvée dans [3], article sur lequel nous nous basons principalement pour cette section. Une autre étude détaillée des travaux de Germain concernant le théorème de Fermat est donnée dans [1]. Dans la première sous-section nous décrivons le *Grand Plan* de Germain pour démontrer le théorème. La deuxième sous-section est consacrée au *Théorème des Grandes Tailles des Solutions* de Germain, duquel découlera le théorème qui est aujourd'hui connu sous le nom de *Théorème de Sophie Germain*.

3.1 Le Grand Plan

Dans cette sous-section nous considérons le plan complet de Germain avec lequel elle espérait démontrer le théorème de Fermat. Pour cela elle démontre tout d'abord un théorème de base qui reviendra dans tous ses travaux. Pour ce théorème, elle utilisera la condition dite de *non-consécutivité* (condition N-C).

Condition (N-C). Il n'y a pas deux résidus p-ième puissance consécutifs modulo θ.

Avec ceci elle établit son théorème de base comme suit.

Théorème 6. *Si l'équation $x^p + y^p = z^p$ admet une solution en nombres entiers, alors tout nombre premier θ de la forme $2np + 1$, avec $n \in \mathbb{N}$, qui satisfait N-C, divise x, y ou z.*

Avant de démontrer le théorème de base, nous considérons un exemple afin de clarifier la condition N-C. Considérons le nombre premier $p = 5$ et considérons $1 \leq n \leq 10$. Nous nous demandons d'abord si le nombre $\theta = 2np + 1$ est premier et, le cas échéant, s'il satisfait la condition N-C. Définissons l'ensemble R comme étant l'ensemble des résidus p-ième puissance modulo θ, c.-à-d. $R = \{x^p \pmod{\theta} \mid 1 \leq x \leq \theta - 1\}$. Les résultats pour $1 \leq n \leq 10$ sont montrés dans la table 1.

La table 1 montre que pour $p = 5$ la condition N-C est satisfaite pour au moins $\theta = 11, 41, 71, 101$. Considérons donc maintenant la preuve du théorème 6.

n	θ	R	N-C	P-P-P
1	11	$R=\{1,10\}$	√	√
2	21	θ pas premier	×	×
3	31	$R=\{1,5,6,25,26,30\}$	×	×
4	41	$R=\{1,3,9,14,27,32,38,40\}$	√	√
5	51	θ pas premier	×	×
6	61	$R=\{1,11,13,14,21,29,32,40,47,48,50,60\}$	×	√
7	71	$R=\{1,20,23,26,30,32,34,37,39,41,45,48,51,70\}$	√	√
8	81	θ pas premier	×	×
9	91	$R=\{1,2,4,5,\ldots,86,87,89,90\}$	×	×
10	101	$R=\{1,6,10,14,17,\ldots 84,87,91,95,100\}$	√	√

TABLE 1 — Illustration pour $p=5$ et $1\leq n\leq 10$.

Démonstration. Supposons que x, y et z satisfassent l'équation $x^p+y^p=z^p$. Soit θ de la forme $2np+1$ et tel que θ satisfait N-C. Supposons que θ ne divise ni x, ni y, ni z. Alors $x^p+y^p=z^p$ et ceci équivaut à $z^p-y^p=x^p$. Modulo θ l'équation reste valable et, comme θ est premier et ne divise aucun des trois nombres entiers x, y, z, on peut diviser l'équation par x^p. Après division par x^p on obtient

$$\left(\frac{z}{x}\right)^p-\left(\frac{y}{x}\right)^p\equiv 1 \mod \theta.$$

Or ceci signifie que les nombres $\left(\frac{z}{x}\right)$ et $\left(\frac{y}{x}\right)$, si on les considère comme entiers modulo θ, sont des p-ièmes puissances consécutives modulo θ, ce qui contredit le fait que θ satisfait N-C. □

La prochaine étape dans la quête de Germain pour une preuve du théorème de Fermat était de démontrer que pour tout nombre premier p, il existait une infinité de nombres premiers θ, de la forme $2np+1$, satisfaisant N-C. Ceci aurait alors comme corollaire presque immédiat la preuve du théorème de Fermat. En effet, supposons que $x^p+y^p=z^p$ admette une solution en nombres entiers X, Y et Z. Il existe alors une infinité de nombres premiers θ satisfaisant N-C et, par le théorème 6, chacun de ces nombres premiers θ divise X, Y ou Z. Or ceci signifie que au moins un de ces trois nombres est divisible par une infinité de nombres premiers θ, ce qui est bien sûr impossible.

Une question qu'on se pose en analysant les manuscrits de Germain est pourquoi elle ne considère que des nombres premiers θ de la forme $2np+1$. La réponse est qu'elle était probablement bien consciente du lemme suivant.

Lemme 7. *Soient p et q deux nombres premiers tels que* $\operatorname{pgcd}(p,q-1)=1$. *Alors il existe deux nombres entiers x et y tels que* $x^p-y^p\equiv 1 \pmod q$.

Démonstration. Soient p et q comme dans l'énoncé du lemme. Alors par le théorème de Bézout, il existe deux entiers a et b tels que $ap+b(q-1)=1$. Choisissons deux nombres entiers x_0 et y_0 tels que $x_0-y_0\equiv 1 \pmod q$. Alors $x_0=x_0^{ap+b(q-1)}$ et modulo q on obtient $x_0\equiv x_0^{ap}\left(x_0^{q-1}\right)^b \pmod q$. Or, par le petit théorème de Fermat (voir le théorème 4), $x_0^{q-1}\equiv 1 \pmod q$ et donc $x_0\equiv\left(x_0^a\right)^p \pmod q$. De la

même manière $y_0 \equiv \left(y_0^a\right)^p \pmod{q}$. Finalement on trouve que $\left(x_0^a\right)^p - \left(y_0^a\right)^p \equiv 1 \pmod{q}$. □

Ceci montre que si le nombre premier θ est tel que $\text{pgcd}(p, \theta - 1) = 1$, alors θ ne vérifie certainement pas N-C. Il suffit donc de considérer des nombres premiers θ tels que $\text{pgcd}(p, \theta) \neq 1$. Or comme p est premier ceci équivaut à considérer des θ tels que $p \mid \theta - 1$. C'est pourquoi Germain ne considère que des nombres premiers θ de la forme $2np + 1$, où le paramètre 2 est dû au fait qu'un nombre premier supérieur à 3 est toujours impair.

Le but est donc maintenant de prouver qu'il existe pour chaque nombre premier p une infinité de nombres premiers θ qui vérifient la condition N-C. Or l'idée de Germain n'est pas de démontrer ceci directement, mais plutôt de démontrer la chose suivante.

Conjecture 8. *Pour tout $n \in \mathbb{N}$, il existe seulement un nombre fini de nombres $p \in \mathbb{N}$ tels que $2np + 1$ ne satisfait pas N-C.*

A première vue, cette conjecture semble « aller dans le mauvais sens ». Or, le plan final de Germain est de démontrer l'existence d'une valeur $K > 0$ telle que pour tout nombre premier $p > K$ le nombre $2np + 1$ soit premier et satisfasse N-C. Ceci impliquerait alors la preuve du théorème de Fermat pour tout nombre premier $p > K$. Malheureusement Germain n'a jamais pu démontrer ce résultat. Par contre elle a effectué, à la main, tous les calculs pour $n \leq 10$ et $2 < p < 100$:

> Je n'ai jamais pu arriver à l'infini quoique j'ai 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 que pour chaque valeur de p il n'existe pas une limite au delà de laquelle tous les nombres de la forme $2np + 1$ auraient deux résidus p-ième puissance placés de suite dans la série des nombres naturels. C'est le cas qui intéresse l'équation de Fermat.

De plus Germain a obtenu un résultat concret pour le cas $n = 1$, qui est le suivant.

Lemme 9. *Soit p un nombre premier. Si $\theta = 2p + 1$ est premier, θ vérifie automatiquement N-C.*

Démonstration. Regardons quels éléments de $\mathbb{Z}_\theta$ s'écrivent comme puissances de p. Soit $a \in \mathbb{Z}_\theta$ une puissance de p. Il existe donc $x \in \mathbb{Z}_\theta$ tel que $x^p \equiv a \pmod{\theta}$. Or par le théorème 5, ceci est possible si et seulement si $a^{\frac{\theta-1}{d}} \equiv 1 \pmod{\theta}$. Dans ce cas $\theta - 1 = 2p$ et $d = p$ et a doit donc être solution de l'équation $y^2 \equiv 1 \pmod{\theta}$. Les seules solutions de cette équation sont 1 et $\theta - 1$ et θ vérifie donc N-C. □

A cause de ce théorème, les nombres premiers p tels que $2p+1$ est aussi premier sont appelés *nombres premiers de Sophie Germain*.

Finalement, le cas qui a vraiment mis en doute Germain concernant sa conjecture a été le cas $p = 3$. En fait Germain a prouvé le lemme suivant, qui démontre l'échec de sa conjecture, au moins pour $p = 3$.

Lemme 10. *Pour chaque nombre premier θ de la forme $6n + 1$ avec $n > 2$, il y a deux résidus troisième puissance consécutifs modulo θ.*

Démonstration. Supposons que θ satisfasse N-C et supposons d'abord qu'il n'existe pas de valeurs $r, r' \in \{1, \ldots, 6n\}$ telles que $r - r' = 2$ et r et r' soient des résidus cubiques. Par le théorème 5 on a

$$x^3 \equiv b \mod 6n+1 \text{ si et seulement si } b^{2n} \equiv 1 \mod 6n+1,$$

et donc il existe exactement $2n$ résidus cubiques modulo $6n+1$. Ceux-ci sont distribués parmi $6n$ valeurs et, à cause de l'hypothèse de départ, entre deux résidus cubiques il y a toujours une différence d'au moins 2. Les $4n$ résidus non cubiques sont donc distribués parmi les $2n-1$ « trous ». Comme chaque trou comporte au moins 2 résidus non cubiques, on a déjà sûrement $4n-2$ des $4n$ résidus non cubiques qui sont distribués dans les trous. Il reste 2 résidus non cubiques à répartir. Du coup tous les trous contiennent 2 résidus non cubiques, à part deux trous qui en contiennent 3, respectivement un trou qui en contient 4. Indépendemment de la valeur de $n > 2$, $1 = 1^3$ et $8 = 2^3$, sont résidus cubiques et donc 2 et 3 sont résidus non cubiques. Si 4 était résidu cubique, alors $\frac{8}{4} = 2$ serait résidu cubique aussi. Donc 4 est aussi résidu non cubique. Par conséquent 5 ou 6 sont résidus cubiques. Or, il est facile de voir que les résidus cubiques sont distribués symétriquement parmi les $6n$ valeurs de 1 à $6n$. Par conséquent, si 6 est résidu cubique, le premier trou contient 4 valeurs et par symétrie le dernier en contient 4 aussi, ce qui donne trop de résidus non cubiques. Donc 5 est résidu cubique et la liste des résidus cubiques parmi les valeurs de 1 à $6n$ est la suivante :

$$1,\ 5,\ 8,\ 11,\ \ldots,\ 6n-7,\ 6n-4,\ 6n.$$

Si $n > 5$ alors $\theta > 31$ et, dans ce cas, $27 = 3^3$ est résidu cubique. Or clairement 27 n'est pas dans la liste ci-dessus. Si $\theta < 31$, alors $\theta = 19$ ($\theta = 25$ n'est pas premier) et dans ce cas $7 \equiv 64 \equiv 4^3 \pmod{19}$ et 7 n'est pas non plus dans la liste.

Donc il existe forcément deux résidus cubiques $r, r' \in \{1, \ldots, 6n\}$ tels que $r - r' = 2$. Soit x un générateur du groupe cyclique $\mathbb{Z}_\theta^*$. Alors $2 \equiv x^{3f \pm 1} \pmod{\theta}$, pour $f > 0$. En effet 2 n'est pas un résidu cubique, car 1 en est un et θ satisfait N-C. Considérons $r + r'$. On a $r + r' \not\equiv 0 \pmod{\theta}$, car sinon $2 = r - r' \equiv r - (-r) \equiv 2r \pmod{\theta}$, ce qui implique que $r = 1$. Or $r - r' = 2$ avec $r = 1$ et r et r' positifs est impossible. Donc $r + r' \in \mathbb{Z}_\theta^*$, d'où $r + r' \equiv x^m \pmod{\theta}$ pour $m > 0$. Si $3 \mid m$, alors on a

$$r + r' \equiv \left(x^{m'}\right)^3 \mod \theta$$
$$\Rightarrow r - (-r') \equiv \left(x^{m'}\right)^3 \mod \theta,$$

et en posant $r = q^3$ et $r' = q'^3$ pour $q, q' \in \mathbb{Z}_\theta^*$, cette dernière ligne nous donne $\left(\frac{q}{x^{m'}}\right)^3 - \left(\frac{q'}{x^{m'}}\right)^3 \equiv 1 \pmod{\theta}$, ce qui contredit le fait que θ satisfait N-C. Par conséquent $r + r' \equiv x^{3g \pm 1} \pmod{\theta}$ avec $g > 0$. Supposons que le signe de $3g \pm 1$ soit différent de celui de $3f \pm 1$, c.-à-d. supposons que $2 \equiv x^{3f \pm 1} \pmod{\theta}$ et $r + r' \equiv x^{3g \mp 1} \pmod{\theta}$. Alors

$$r^2 - r'^2 = (r + r')(r - r') \equiv x^{3g \mp 1} x^{3f \pm 1} \equiv \left(x^{g+f}\right)^3 \mod \theta.$$

Comme r et r' sont résidus cubiques, r^2 et r'^2 sont résidus cubiques aussi et la dernière ligne mène de nouveau à une contradiction avec le fait que θ satisfait

N-C. Finalement on a donc que

$$\begin{aligned} 2r = r + r' + r - r' &\equiv x^{3g\pm 1} + x^{3f\pm 1} \mod \theta \\ \Rightarrow x^{3f\pm 1} r &\equiv x^{3g\pm 1} + x^{3f\pm 1} \mod \theta \\ \Rightarrow r &\equiv 1 + x^{3(g-f)} \mod \theta \\ \Rightarrow r - x^{3(g-f)} &\equiv 1 \mod \theta, \end{aligned}$$

ce qui est à nouveau en contradiction avec le fait que θ satisfait N-C. □

Ce lemme montre donc clairement que N-C n'est jamais vérifié si $p = 3$, à part pour $\theta = 7$ et $\theta = 13$. Sur base de ce lemme, Germain décide alors d'abandonner son Grand Plan. Aujourd'hui encore, on ne sait pas si pour p premier il existe toujours un nombre premier θ de la forme $2np + 1$ et qui satisfait N-C. Or malgré l'échec du Grand Plan, la démarche de Germain reste remarquable pour son temps. En fait en voulant démontrer l'existence de cette valeur K au-delà de laquelle $2np + 1$ est premier et satisfait N-C, pour chaque $p > K$ premier, Germain aurait démontré le théorème de Fermat pour chaque exposant premier p supérieur à une certaine valeur K, dont l'existence est prouvée, mais la valeur exacte n'est pas connue. Elle aurait donc démontré le théorème de Fermat pour une infinité d'exposants sans l'avoir démontré pour un seul exposant précis. Ceci constitue une première dans l'histoire du théorème de Fermat car jusqu'ici les mathématiciens avaient toujours essayé de démontrer le théorème pour une valeur précise (d'abord 4, puis 3, puis 5 etc.).

3.2 Théorème des Grandes Tailles des Solutions

Bien que Germain décide d'abandonner son Grand Plan, elle n'arrête pas le travail sur le théorème de Fermat. Dans une deuxième étape elle travaille sur un théorème, qu'on appelle *Théorème des Grandes Tailles des Solutions*. Pour cela elle réutilise la condition N-C et ajoute une deuxième condition, qu'elle appelle *condition P-P-P*, où *P-P-P* représente *p pas une p-ième puissance*.

Condition (P-P-P)**.** Le nombre premier p n'est pas un résidu p-ième puissance modulo θ.

Dans la table 1, on voit que pour $p = 5$ et $1 \leq n \leq 10$, la condition P-P-P est satisfaite pour $\theta = 11, 41, 71, 101$. Avec cette condition, Germain essaie de démontrer le théorème suivant :

Conjecture 11. *Soit p un nombre premier. Si l'équation $x^p + y^p = z^p$ admet une solution en nombres entiers, alors $x + y$, $z - y$ ou $z - x$ doit nécessairement être un multiple de la $(2p-1)$-ième puissance de p ainsi que des p-ièmes puissances de tous les nombres premiers θ de la forme $2np + 1$ qui satisfont N-C et P-P-P.*

L'idée de Sophie Germain derrière ce Théorème des Grandes Tailles des Solutions n'est plus de démontrer le théorème de Fermat directement, mais de démontrer que si l'équation $x^p + y^p = z^p$ a une solution, cette solution doit être gigantesque en taille. Germain écrit à ce sujet les lignes suivantes :

> Vous concevrez aisément, Monsieur, que j'ai dû parvenir à prouver que cette équation ne serait possible qu'en nombres dont la grandeur effraye l'imagination…

En d'autres mots, ce théorème, s'il était vrai, montrerait que parmi les « petits » nombres, il n'y aurait pas de solution à l'équation de Fermat. Considérons un exemple concret. Si ce théorème était vrai, cela signifierait, pour l'exemple de $p = 5$, que $x + y$, $z - y$ ou $z - x$ serait multiple de

$$5^9 \cdot 11^5 \cdot 41^5 \cdot 71^5 \cdot 101^5$$
$$(= 691\,053\,006\,763\,356\,095\,514\,121\,490\,614\,455\,078\,125).$$

On peut montrer que ceci équivaut à ce qu'un des trois nombres contienne au moins 39 chiffres.

Malheureusement Germain fait une faute dans la démonstration du théorème. En ne considérant la preuve que jusqu'au point où se trouve la faute, on peut en déduire le théorème suivant, qu'on appelle encore aujourd'hui *Théorème de Sophie Germain*.

Théorème de Sophie Germain. *Soit p un nombre premier. S'il existe un nombre premier θ de la forme $2np + 1$ qui satisfait les conditions N-C et P-P-P, alors dans toute solution de l'équation $x^p + y^p = z^p$ un des nombres x, y ou z est divisible par p^2.*

Démonstration. Supposons qu'il existe $\theta = 2np + 1$ qui satisfait N-C et P-P-P et supposons que x, y et z satisfassent l'équation $x^p + y^p = z^p$. Alors par le théorème 6, $\theta \mid x, y$ ou z et on va montrer que ce dernier est aussi divisible par p^2. Pour ceci on va démontrer d'abord que les couples suivants

$$\begin{aligned} &x + y \text{ et } \varphi(x,y) = x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \dots \\ &z - y \text{ et } \psi(z,y) = z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + \dots \\ &z - x \text{ et } \psi(z,x) = z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \dots \end{aligned} \tag{1}$$

ne peuvent avoir d'autres diviseurs communs que le nombre p. En effet supposons que q soit un nombre premier différent de p et que $q \mid x + y$ et $q \mid \varphi(x,y)$. Alors $y \equiv -x \pmod q$ et donc $\varphi(x,y) \equiv px^{p-1} \pmod q$. Or comme q divise $\varphi(x,y)$, on a $q \mid px^{p-1}$ ce qui implique que $q \mid x^{p-1}$. Comme q est premier, q divise donc x. Or q divise aussi $x + y$ et donc q divise y. Ceci est en contradiction avec le fait que x, y et z sont premiers entre eux. De même, on peut montrer que les deux autres couples n'ont pas de diviseur commun $q \neq p$ et que les trois couples n'ont pas de diviseur commun égal à une puissance de p.

Supposons maintenant que x, y et z soient premiers à p et posons

$$\begin{aligned} z &= lr, \\ x &= hn, \\ y &= vm, \end{aligned} \tag{2}$$

pour l, r, h, n, v et m des entiers positifs. Comme les produits des couples en (1) sont z^p, x^p et y^p respectivement et comme les couples sont premiers entre eux,

$$\begin{aligned} &x + y = l^p \text{ et } \varphi(x,y) = r^p, \\ &z - y = h^p \text{ et } \psi(z,y) = n^p, \\ &z - x = v^p \text{ et } \psi(z,x) = m^p. \end{aligned} \tag{3}$$

Par le théorème 6, on sait que θ divise x, y ou z. Supposons que $\theta \mid z$ (les autres cas étant analogues). Alors

$$l^p + h^p + v^p \equiv 2z \equiv 0 \mod \theta.$$

Si aucun des trois termes est nul, ceci équivaut à $l^p + h^p \equiv (-v)^p \pmod{\theta}$. Or la dernière équation peut être réécrite comme $\left(\frac{l}{-v}\right)^p + \left(\frac{h}{-v}\right)^p \equiv 1 \pmod{\theta}$ ce qui est en contradiction avec la condition N-C. Donc un des trois termes l^p, h^p ou v^p est divisible par θ. Comme x, y et z sont premiers entre eux, la seule possibilité est que $\theta \mid l$. Donc $x + y \equiv 0 \pmod{\theta}$, ce qui équivaut à

$$\varphi(x, y) \equiv p x^{p-1} \equiv r^p \mod \theta. \tag{4}$$

Comme $z \equiv 0 \pmod{\theta}$ et comme $z - x = v^p$, on a, modulo θ, $x \equiv (-v)^p \pmod{\theta}$. Or en remplaçant x par $(-v)^p$ dans (4), on obtient

$$p\left((-v)^{p-1}\right)^p \equiv r^p \mod \theta,$$

et donc p doit être une p-ième puissance modulo θ, ce qui contredit P-P-P. Ceci implique donc que p divise x, y ou z. Supposons donc que p divise z. Remarquons ici que les autres cas se traitent de manière analogue et que le fait qu'on ait aussi supposé que $\theta \mid z$ ne joue ici plus aucun rôle. Or si $p \mid z$, la première ligne dans (2) et (3) change. Comme $x + y$ et $\varphi(x, y)$ n'ont pas d'autre diviseur commun que p, il y a 4 possibilités :

$$\begin{aligned} x + y = l^p p^p \text{ et } \varphi(x, y) = r^p, \\ x + y = l^p \text{ et } \varphi(x, y) = r^p p^p, \\ x + y = l^p p \text{ et } \varphi(x, y) = r^p p^{p-1}, \\ x + y = l^p p^{p-1} \text{ et } \varphi(x, y) = r^p p. \end{aligned}$$

On peut aisément démontrer que si l'un des deux termes est divisible par p, l'autre l'est aussi et les deux premières possibilités sont donc exclues. Supposons que la troisième possibilité soit vraie et posons $x + y = s$. Alors

$$\varphi(x, y) = \frac{(s - x)^p + x^p}{s} = s^{p-1} - \binom{p}{1} s^{p-2} x + \ldots - \binom{p}{p-2} s x^{p-2} + \binom{p}{p-1} x^{p-1}.$$

Dans cette expression chaque terme est divisible par au moins p^2, à part le dernier qui est juste divisible par p. Ceci contredit le fait que $\varphi(x, y)$ est divisible par plus que p et c'est donc la quatrième possibilité qui est vraie. Donc p divise aussi $2z - x - y$ qui est égal à $h^p + v^p$. Ceci donne

$$\begin{aligned} & h^p + v^p \equiv 0 \mod p \\ \Rightarrow & h^{p-1} h + v^{p-1} v \equiv 0 \mod p \\ \Rightarrow & h + v \equiv 0 \mod p \\ \Rightarrow & h \equiv -v \mod p. \end{aligned}$$

Or $h^p + v^p = (h + v)\varphi(h, v)$ et le premier terme est divisible par p et le deuxième peut être écrit modulo p comme $p h^{p-1}$ et est donc aussi divisible par p. Donc $p^2 \mid h^p + v^p$ et donc $p^2 \mid 2z - x - y$. Or $x - y$ est aussi divisible par p^2 et donc z doit être divisible par p^2, ce qui conclut la démonstration. □

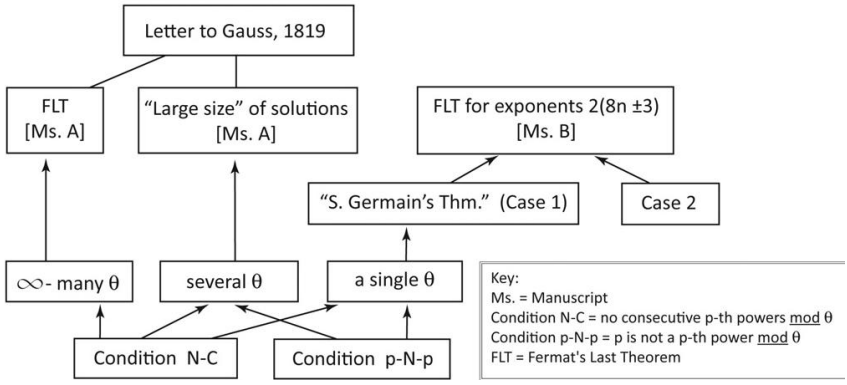

FIGURE 3 — Schéma du travail complet de Germain sur le théorème de Fermat (tiré de l'article [3])

Le théorème de Sophie Germain est aujourd'hui utilisé en théorie des nombres. En plus il démontre une partie du théorème de Fermat. En fait la démonstration du théorème de Fermat de Andrew Wiles est divisée en deux cas :

- L'équation $x^p + y^p = z^p$ n'a pas de solution en nombres entiers tels que $p \nmid xyz$.
- L'équation $x^p + y^p = z^p$ n'a pas de solution en nombres entiers tels que un et un seul des nombres x, y ou z soit divisible par p.

En fait le théorème de Sophie Germain démontre le cas 1 pour

- tous les nombres premiers p tels que $p < 100$,
- les nombres premiers de Sophie Germain (voir en-dessous de la démonstration du lemme 9).

Pour conclure le travail de Germain, la figure 3 montre un résumé de son travail. Quelques éléments n'ont pas été traités dans ce texte. Les lecteurs souhaitant plus d'information sur cette partie de ses travaux sont invités à consulter [3].

4 Les nombres premiers de Sophie Germain

Rappelons tout d'abord la définition d'un nombre premier de Sophie Germain.

Définition 12. Les nombres premiers p tels que $2p + 1$ est aussi premier sont appelés nombres premiers de Sophie Germain.

4.1 Les nombres premiers de Sophie Germain dans la recherche

Jusqu'à aujourd'hui la conjecture suivante n'a pas été résolue.

Conjecture 13. *Il y a une infinité de nombres premiers de Sophie Germain.*

Le plus grand nombre premier de Sophie Germain a été trouvé en mars 2010 et correspond à

$$183027 \cdot 2^{265440} - 1,$$

ce qui représente un nombre à 79 911 chiffres.

Dans la recherche contemporaine les nombres premiers de Sophie Germain trouvent leur application principale en cryptographie, et plus précisément dans le domaine des signatures digitales.

4.2 Nombres premiers de Sophie Germain palindromiques

Rappelons d'abord qu'un nombre est appelé palindromique lorsque son écriture décimale lue de gauche à droite ou de droite à gauche représente le même nombre. Par exemple 22, 151, 6446 ou 12 345 678 987 654 321 sont des nombres palindromiques. Harvey Dubner, un ingénieur américain retraité, s'amuse à trouver des grands nombres premiers de Sophie Germain qui sont palindromiques. En ce moment il tient le record du plus grand nombre de Sophie Germain palindromique qui est le suivant :

$$10\ldots05321812350\ldots01,$$

où les pointillés ci-dessus représentent à chaque fois 516 fois le chiffre 0 !

Bien que ceci ait déjà l'air fort impressionnant, notre ingénieur a trouvé mieux. En effet, il a trouvé un nombre premier de Sophie Germain P tel que $Q = 2P+1$ est aussi un nombre premier de Sophie Germain. Donc $R = 2Q + 1$ est aussi premier et les trois nombres sont palindromiques. Les voici :

- $P = 1\,919\,191\,918\,090\,908\,081\,808\,090\,908\,191\,919\,191$
- $Q = 2P + 1 = 3\,838\,383\,836\,181\,816\,163\,616\,181\,816\,383\,838\,383$
- $R = 2Q + 1 = 7\,676\,767\,672\,363\,632\,327\,232\,363\,632\,767\,676\,767$

On peut démontrer que la plus longue suite ainsi possible est toujours une suite de 3 nombres. Or notre ingénieur a encore trouvé mieux et ici aussi il détient le record de la plus grande suite de ce type, qui est montrée dans la figure 4.

En plus du fait que cette suite soit formée par les nombres les plus longs, elle a encore autre chose de remarquable. Chacun des trois nombres dans cette suite a exactement 727 chiffres et 727 est, à nouveau, un palindrome ! Et si, à la lecture de ces lignes, vous souriez, c'est qu'il doit y avoir un peu de cette extraordinaire mathématicienne en vous !

```
P =
1818181808080818080808180818081818081808181818081808080818180808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080808080808080808080808080808080808_
0808080808080808080808080808080808080818180808081808181818081808181808_
1808180808081808080818181811

Q =
3636363616161636161616361636163616361636163636361636161616363616161616_
1616161616161616161616161616161616161616161616161616161616161616161616_
1616161616161616161616161616161616161616161616161616161616161616161616_
1616161616161616161616161616161616161616161616161616161616161616161616_
1616161616161616161616161616161616161616161616161616161616161616161616_
1616161616161616161616161616161616161616161616161616161616161616161616_
1616161616161616161616161616161616161616161616161616161616161616161616_
1616161616161616161616161616161616161616161616161616161616161616161616_
1616161616161616161616161616161616161616161616161616161616161616161616_
1616161616161616161616161616161636361616163616363636163616363616_
3616361616163616161636363

R =
7272727232323272323232723272327272327232727272327232323272723232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232323232323232323232323232323232_
3232323232323232323232323232323232323232727232323272327272723272327232_
7232723232327232323272727
```

Figure 4 — Suite la plus grande connue (tirée de la page web [5])

5 Bibliographie

[1] A. Del Centina, *Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's last theorem*, Arch. Hist. Exact Sci., 62 (2008), pp. 349–392.

[2] D. Ford and V. Jha, *On Wendt's determinant and Sophie Germain's theorem*, Experiment. Math., 2 (1993), pp. 113–120.

[3] R. Laubenbacher and D. Pengelley, *"Voici ce que j'ai trouvé :" Sophie Germain's grand plan to prove Fermat's last theorem*, Historia Math., 37 (2010), pp. 641–692.

[4] J. Navarro, *Les Femmes et les Mathématiques*, RBA, 2012.

[5] L. Riddle, *Sophie germain and fermat's last theorem*. `http://www.agnesscott.edu/lriddle/women/germain-flt/sgandflt.htm`.

[6] S. Singh, *Fermat's Last Theorem*, Harper Perennial, 2007.