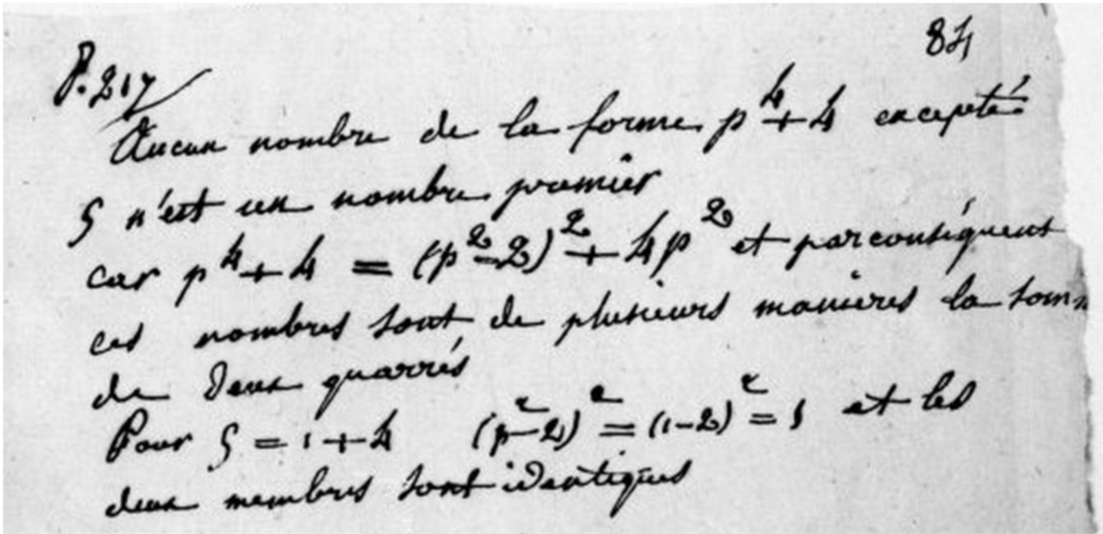
THEOREM OF THE DAY

Sophie Germain's Identity *The expression $x^4 + 4y^4$ factorises as*

$$x^4 + 4y^4 = \left((x+y)^2 + y^2\right)\left((x-y)^2 + y^2\right) = \left(x^2 + 2xy + 2y^2\right)\left(x^2 - 2xy + 2y^2\right).$$

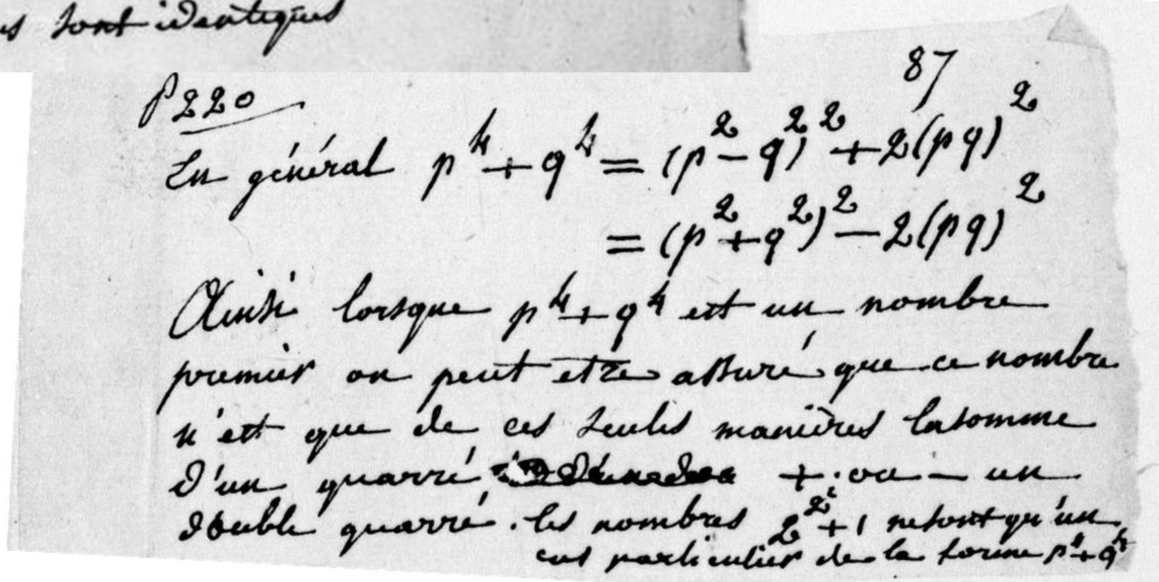
Sophie Germain (1778–1835)



84

p. 217

Aucun nombre de la forme p^4+4 excepté
5 n'est un nombre premier
car $p^4+4 = (p^2-2)^2+4p^2$ et par conséquent
ces nombres sont de plusieurs manières la somme
de deux quarrés
Pour $5 = 1+4$ $(p^2-2)^2 = (1-2)^2 = 1$ et les
deux membres sont identiques



87

p. 220

En général $p^4+q^4 = (p^2-q^2)^2+2(pq)^2$
$= (p^2+q^2)^2-2(pq)^2$
Ainsi lorsque p^4+q^4 est un nombre
premier on peut être assuré que ce nombre
n'est que de ces seules manières la somme
d'un quarré + ou − un
double quarré. Les nombres $2^{2^i}+1$ ne sont qu'un
cas particulier de la forme p^4+q^4

Manuscript source: gallica.bnf.fr/Bibliothèque nationale de France

A transliteration being: "Aucun nombre de la forme $p^4 + 4$ excepté 5 n'est un nombre premier, car $p^4 + 4 = (p^2 - 2)^2 + 4p^2$ et par conséquent ces nombres sont de plusiers manières la somme de deux carrés." ("No number of the form $p^4 + 4$ except 5 is a prime number, because $p^4 + 4 = (p^2 - 2)^2 + 4p^2$ and consequently these numbers are representable in more than one way as a sum of two squares"). Sophie Germain is appealing here to the uniqueness of the representation in Fermat's Two-Squares Theorem.

And the subsequent text: "En général $p^4 + q^4 = \left(p^2 - q^2\right)^2 + 2(pq)^2 = \left(p^2 + q^2\right)^2 - 2(pq)^2$. Ansi lorsque $p^4 + q^4$ est un nombre premier on peut être assuré que ce nombre n'est que de ces seules manières la somme d'un carré + ou − un double carré. Les nombres $2^{2^i} + 1$ ne sont q'un cas particulier de la forme $p^4 + q^4$." ("Thus when $p^4 + q^4$ is a prime one is sure that the number is only thus expressible as the sum of a square + or − twice a square. The numbers $2^{2^i} + 1$ are just a special case of the form $p^4 + q^4$.") The special case in question is that of the *Fermat numbers* whose primality in general was disproved by Euler in 1732 and which have remained a subject of research ever since.

Germain does not (here) assert her Identity, but it follows at once from the modification $p^4 + 4q^4 = \left(p^2 + 2q^2\right)^2 - 4(pq)^2$ by factorising the difference of two squares. In any case it is a trivial verification. But it is a 'trick' which reveals numerous truths in elementary number theory. For example, try this: prove that $3^r + 4^s = 5^t$ has only two solutions in nonnegative integers r, s, t, namely $r = s = t = 2$ and $r = 0, s = t = 1$.

The attribution of this identity to Sophie Germain is by L.E. Dickson who cites p.84 of manuscript 9118 in the collection of the Bibliotèque nationale de France. As we have seen the attribution is not exact. Dickson locates the same identity in a letter from Euler to Goldbach in 1742 but is again inexact; the letter (28th August) gives only the special case $1 + 4x^4 = (2x^2 + 2x + 1)(2x^2 - 2x + 1)$. Certainly the Identity and its applications are very much in the spirit of Germain's ingenious and pioneering work in number theory.

Web link: cms.math.ca/crux/v26/n7/page417-428.pdf, pp. 426–428, is the source of the application to $3^r + 4^s = 5^t$.

Further reading: *History of the Theory of Numbers, Volume I* by L.E. Dickson, Dover reprint edition, 2005.