BO1.1. HISTORY OF MATHEMATICS
HT26 READING COURSE:
THE QUEST FOR FERMAT'S LAST THEOREM

Letter from Sophie Germain to Carl Friedrich Gauss, 12 May 1819: Translated from the French text transcribed by Andrea Del Centina and Alessandra Fiocca, 'The correspondence between Sophie Germain and Carl Friedrich Gauss', *Archive for History of Exact Sciences* 66 (2012), 585–700 (689–693); the notes at the end of this translation are adapted from the latter article.

Paris (Rue de Braque n.4) 12 May 1819

Sir,

I very much regret that you did not accompany your friend; I would have had the greatest pleasure in hearing you speak of the beautiful theories which are the subject of your favourite studies and for which I myself have a real passion.

The new demonstrations contained in your memoir have enchanted me.[1] You seem to prefer the latter because of the connection it establishes between truths which at first glance seem to be independent. I was undoubtedly very sensitive to this kind of surprise which several places in the *disquisitions* had already made me experience. However, I admit that the statement of theorem no. 2 pleased me even more. This sentence which ends it: *Tunc tres numeri n, N, $1/4(m-1)(N-1)$, vel omnes simul pares erunt, vel unus par duoque reliqui impares* [*Then the three numbers n, N, $1/4(m-1)(N-1)$ will either all be even, or one will be even and the other two odd*] struck me with a kind of admiration somewhat contrary to that of which I have just spoken because one feels the entire demonstration there and for this reason it seems to me to have reached the highest degree of elegance that one can imagine.

It is always with a new interest that we consider different points of view of the same truth: the entirely new applications that you make of the fundamental theorem to the determination of the question of residue or non-residue presents another kind of enjoyment: it is a real acquisition which can be of great use.

I regret that you have been putting off giving us your research on cubic and biquadratic residues for so long. By dealing with these questions, it is likely that you would have the means to go even further, I mean to extend the theory to residues of any power.

I have not yet had the time to read the memoir on attractions;[2] I intend to study it because this subject is much less familiar to me than the theory of residues. I wanted to reserve for myself, before the departure of your friend, the time to thank you as I owe you and also to communicate to you the research that has occupied me since the time when I had the honour of writing to you.

Although I have worked for some time on the theory of vibrating surfaces (to which I would have much to add if I had the reason to carry out the experiments I have imagined concerning cylindrical surfaces), I have never ceased to think about the theory of numbers. I will give you an idea of my preoccupation with this kind of research by admitting that even without any expectation of success I prefer it to work which would necessarily give me a result and which nevertheless interests me . . . when I think about it.

Long before our academy proposed as a prize subject the demonstration of the impossibility of Fermat's equation, this kind of challenge to modern theories by a geometer who was deprived of the resources we possess today, often tormented me. I vaguely glimpsed a connection between the theory of residues and the famous equation, I even believe you spoke of this idea previously because it struck me as soon as I became aware of your book.

Here is what I have found:

The order in which the residues (powers equal to the exponent) are placed in the series of natural numbers determines the necessary divisors which belong to the numbers between which we establish not only Fermat's equation but also many other equations analogous to it.

Let us take for example Fermat's own equation, which is the simplest of all those discussed here.

So, p being a prime number, $z^p = x^p + y^p$.

I say that if this equation is possible, any prime number of the form $2Np + 1$ (N being any integer) for which there are not two residues of the p-th power placed in a row in the series of natural numbers will necessarily divide one of the numbers x, y and z.

This is obvious, because the equation $z^p = x^p + y^p$ gives the congruence $1 \equiv r^{sp} - r^{tp}$ in which r represents a primitive root and s and t are integers.

We know that the equation has infinitely many solutions when $p = 2$. And indeed all numbers except 3 and 5 have at least two square residues whose difference is unity. Also in this case the known form $h^2 + f^2$, $2fh$, $h^2 - f^2$ of the numbers z [x], y and z shows that one of these numbers is a multiple of 3 and also that one of the same numbers is a multiple of 5.

It is easy to see that if any number k is a p-th power residue mod $2Np + 1$ and there are two p-th power residues of the same mod whose difference is unity, there will also be two p-th power residues whose difference will be k.

But it can happen that we have two p-th residues whose difference is k, without k being a p-th residue.

That being said, here is the general equation whose solution seems to me to depend, like Fermat's, on the order of the residues:

$$kz^n = x^p \pm y^p$$

for from what has just been said we see that every prime number of the form $2Np + 1$ for which two p-th residues do not differ by k divides the number z [one of the numbers x, y, z]. It follows from this that if there were an infinite number of such numbers the equation would be impossible.

I have never been able to reach infinity, although I have pushed the limits far back by a method of trial and error that is too long for me to be able to explain it here. I would not even dare to assert that for each value of p there does not exist a limit beyond which all numbers of the form $2Np + 1$ would have two p-th residues placed in a row in the series of natural numbers. This is the case that interests Fermat's equation.

You will easily understand, Sir, that I had to succeed in proving that this equation would only be possible in numbers whose magnitude frightens the imagination; because it is still subject to many other conditions that I do not have the time to examine because of the details necessary to establish its reality. But all this is still nothing, we need the infinite and not the very large.

Along the way I helped myself with a system of six congruences, any one of which gives the other five. When for a number of the form $2Np + 1$, 2 is not a p-th power residue and at the same time N is prime to 3, the six congruences are not reducible to a lesser number. We can then be sure (n being a different integer for each value of $2Np + 1$) that there are always $6n$ p-th residues (mod $2Np + 1$) placed two by two close to each other in the series of natural numbers. I have made a great deal of effort to find the cases in which $n = 0$. The method I have employed shows that the number of conditions to be fulfilled so that n is not zero depends on the value of

N in the number $2Np+1$ which we take as the modulus: it is perfectly independent of that of p (consequently [in] everything that follows p no longer represents exclusively prime numbers but any integers, this is evident from the examples I will cite later) so that every time I calculated values of N for which $2N+1$ or $4N+1$ were prime I always found a way to fulfil the required conditions. This must be true since there are always two power residues placed in a row in the series of natural numbers and except for 3 and 5 there are also always two square residues placed in a row.

When N is not too large we only have a small number of conditions to try and if we do not find any number that satisfies them we can be sure that whatever p is we never have two p-th residues (mod $2Np+1$) placed in a row in the series of natural numbers.

The method gives all the values of p for which there are two residues that follow each other, it also gives for each value of p the totality of cases where a p-th residue is followed by a similar residue. It gives with equal ease the cases where the interval which separates two p-th residues is k but if k is > 1 the system of six congruences no longer holds. This method has no other disadvantage than the length when N is a little large. In truth certain computational artifices which present themselves naturally can shorten it a little. Moreover, the calculations which it requires are extremely simple and easy.

Here are some examples taken from an old note that I don't have time to check:

Excluding $p = 1$ and $p = 2$, we find that no prime number of the forms $4p+1$, $8p+1$ can have two p-th residues whose difference is unity; that the only prime number of the form $10p+1$ that has two consecutive residues is $10 \cdot 3 + 1$; that the only numbers of the form $14p+1$ that have two consecutive residues are $14 \cdot 3 + 1$ and $14 \cdot 9 + 1$; that the only number of the form $16p+1$ that has two consecutive residues is $16 \cdot 16 + 1$; that the only number of the form $20p+1$ that has two consecutive residues is $20 \cdot 16 + 1$.

I suppose you have before you Mr. Poinsot's dissertation, or rather draft dissertation, since one must do oneself the work that the author spared himself.[3] Be that as it may, his idea struck me as very fortunate. I admired how, starting from such different principles, he had, in a way, provided me with the metaphysics for my method. Indeed, by making use of this author's remark, one can see how I arrived at the results I have just presented, since it concerns the roots of the binomial equation of degree $2N$, and although the quantities resulting from the combination of these roots (or, what amounts to the same thing, and is more in keeping with the method I have used, the combination of their powers) can only become real for certain values of $2Np+1$ and consequently also of p, their ratios to each other are independent of the values of p.

I also sought to apply Mr. Poinsot's ideas to numbers of the form $2^s p+1$ which gives a binomial equation of order 2^s to solve.

I would have liked to establish a relationship between the values of the roots of this equation and those of the equation of degree $2^{s'}$, which gives the p-th power residues $(\text{mod}\, 2^{s'}p+1)$. If we could find in which cases the number $2^s p+1$ is found among the roots of the equation of order $2^{s'}$, and conversely, in which cases $2^{s'}p+1$ is found among the roots of the equation of order $2^{s'}$, that would be very nice and quite analogous to the fundamental theorem, but I haven't reached that point yet.

Mr. Poinsot's notation has provided me with yet another way to prove that 2 is a square residue of numbers of the form $8n+1$ and not a square residue of those of the form $8n+5$: I don't know why this truth appears in so many different forms. Here it is: $2\sqrt{-1} = (1+\sqrt{-1})^2$, therefore $2\sqrt{-1}$ is a square residue: if the modulus is $8n+1$, $\sqrt{-1}$ is a square residue: if the modulus is $8n+5$, $\sqrt{-1}$ is not a square residue, therefore, etc.

We can also see from this notation that if 2 is a p-th residue $(\bmod 2Np+1)$, where p is an odd number, we will have three consecutive p-th residues in the series of natural numbers. These three residues will be $\sqrt{-1}-1$, $\sqrt{-1}$, $\sqrt{-1}+1$. Indeed, if 2 is a p-th residue, then $\pm 2\sqrt{-1}$, and consequently $(\sqrt{-1}\pm 1)^2$ and $\sqrt{-1}\pm 1$, will similarly be p-th residues, and so on.

I beg your indulgence for the carelessness with which this long letter has been written. I have not had the necessary time to organise my thoughts more thoroughly. I have written freely and from memory, and consequently too loosely. I did not want to miss the opportunity to consult you on the importance that may be attached to the ideas I have the honour of communicating to you. I would be particularly curious to know what you think of the use that can be made of the order in which the p-th residues are placed in the series of natural numbers. I believe this consideration is particular, and I have too little confidence in my judgement to dare to decide whether it deserves to be followed.

I can assure you, Sir, that it was the study of your book that transformed my existing interest in indeterminate analysis into a passion. This is not the place to dwell on the beautiful things it contains; they have been too well appreciated by all who have studied it for me to have anything new to add. Allow me, however, to express how important the simple substitution of congruences represented by the symbol $\equiv$ seemed to me. The notion of equality, formerly indicated by the symbol $=$, always seemed to me to contradict the progress of analysis, and I cannot express how much clarity, and consequently ease, I have found in this branch of calculus, with the help of your notation.

One must have mastered the calculus to sense these things. In truth, with this help, I haven't yet gone very far.

I would be most grateful if you would be kind enough to take the time to tell me what you think of the path I have followed. Whatever your opinion, I will receive it with respect and gratitude.

Please accept, Sir, the assurance of my sincere admiration, with which I have the honour to be

your most humble servant
Sophie Germain

Notes

[1] This refers to: C. F. Gauss, 'Theorematis fundamentalis in doctrina de residuis quadratici demonstrationes et ampliationes novae', *Commentationes S. R. Scientiarum Gottingensis recentiores* 4 (1818).

[2] This probably refers to: C. F. Gauss, 'Theoria attractionis corporum sphaeroidorum ellipticorum homogeneorum methodo nova tractata', *Commentationes S. R. Scientiarum Gottingensis recentiores* 2 (1813).

[3] This refers to: L. Poinsot, 'Extrait de quelques recherches nouvelles sur l'algèbre et la théorie des nombres', *Mémoires Acad. des science de l'Institut de France* 14 (1813–1815), 381–392.

Translated by CHRISTOPHER D. HOLLINGS