BO1.1. History of Mathematics

Sheet 0 — HT26

Reading Course: The quest for Fermat's Last Theorem.

Christmas Vacation Reading

Outline

In this reading course, we will expand upon the few brief comments made during the lecture course on Fermat's Last Theorem. We will look at its origins, some of the earlier attempts to prove it, and the impact that it had on subsequent mathematics.

The basic story of Fermat's Last Theorem is well known: during his number-theoretic investigations, while considering the problem of splitting a given square into a sum of two squares, Pierre de Fermat (1601–1665) made a casual (and infamous) note to the effect that the analogous statement is not true for any higher powers:

> It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.[1]

The modern statement of the result is of course that the equation $x^n + y^n = z^n$ has no positive integer solutions if $n > 2$. Over the following 350 years, efforts were made by many mathematicians to supply the missing proof. Developments were incremental until a complete proof was finally supplied by Andrew Wiles (and Richard Taylor) in the 1990s.

We will go beyond the well-known story by looking first at the origins of Fermat's assertion. The margins in which he was writing were those of his copy of Claude Gaspar Bachet de Méziriac's edition of the *Arithmetica* of Diophantus (fl. 250 CE). As we saw in the lecture course, this is a text that was composed in the 3rd century CE, and consists of problems that we would now label as algebra or number theory. Among these was the problem to which Fermat was responding: to split a square into a sum of two squares, which appears in the *Arithmetica* as Problem 8 of Book 2. Looking at squares in this way is of course closely related to the idea of Pythagorean triples, so as part of our background to Fermat's work, we will also look at the most comprehensive ancient treatment of these, which Diophantus had almost certainly read, namely that found in the *Elements* of Euclid (fl. 300 BCE). In order to help us with Fermat's wider number-theoretic work, we will also look at some of the other things that Euclid had to say on number theory, particularly on perfect numbers.

[1] 'Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & 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.' (*Diophanti Alexandrini Arithmeticorum libri sex, et De numeris multangulis liber vnus: cum commentariis C. G. Bacheti* [...] *& obseruationibus D. P de Fermat* [...] *Accessit Doctrinae analyticae inuentum nouum, collectum ex varijs eiusdem D. de Fermat epistolis* (Samuel de Fermat, ed.), Toulouse, 1670, p. 61)

Christopher Hollings: christopher.hollings@maths.ox.ac.uk

With this background knowledge in place, we will turn our attention next to Fermat's number theory, of which his assertion on what came to be known as the Last Theorem forms just one small part. Fermat's view of Diophantus, in common with the views held more widely in 17th-century Europe of ancient mathematical authors, was that he had hidden many of his methods. Fermat's goal therefore was to attempt to fill the supposed 'gaps' in Diophantus's writings. His work touched upon a range of number-theoretic topics, including perfect numbers and Diophantine equations, and we will read a selection of his writings in order to get a flavour of his views on number theory. In particular, we will study one of the few proofs that Fermat did leave behind: a proof of the Last Theorem for exponent 4.

As we saw in the lecture course, however, Fermat largely failed to interest his contemporaries in number-theoretic investigations, which were widely regarded as pointless numerical tinkering. This attitude began to change in the following century, however, when Leonhard Euler (1707–1783) picked up some of the problems left by Fermat. The latter had never published any of his number-theoretic investigations during his lifetime (though he had communicated some of his ideas to his correspondents), but his son Samuel had published a new version of Bachet's Diophantus with Fermat's notes included. Thus, history repeated itself as Euler set about trying to fill the mathematical gaps left behind by Fermat. With regard to the Last Theorem (so called because it was the result that was left after Euler had provided demonstrations of Fermat's other unproved assertions), Euler published two slightly different proofs for exponent 4: one in a paper written in 1738 (but not published until 1747), and another in his 1770 textbook *Elements of algebra*. Despite years of striving, he never produced a satisfactory proof for exponent 3. Nevertheless, the attention that Euler gave to wider number-theoretic investigations gradually had the effect of turning number theory into a respectable branch of mathematics, something that was reinforced by the appearance of Carl Friedrich Gauss's number-theoretic text *Disquisitiones arithmeticae* in 1801.

Hereafter, progress towards a proof of the Last Theorem was often incremental, dealing only in specific exponents. In the early 19th century, several authors succeeded in filling the gaps in Euler's attempted proofs for exponent 3, and a proof for exponent 5 was arrived at independently by Adrien-Marie Legendre and Peter Gustav Lejeune Dirichlet in the 1820s. But progress was also made towards more general methods. The first of these was due to Sophie Germain (1776–1831), who proved, around 1819, that for a given odd prime exponent p, if there exist nonzero integers x, y, z such that $x^p + y^p = z^p$, and a further prime θ with certain properties, then θ has to divide one of x, y, z. Germain's goal was to show further that for a given p, there are infinitely many θ, in which case one of x, y, z has to be divisible by infinitely many primes— an absurdity that then proves Fermat's Last Theorem for exponent p. Although Germain was ultimately unsuccessful in this wider programme of research, some of the techniques that she developed were central to later attacks on the Last Theorem. She never published her ideas, but did communicate some of them in her letters to Gauss. We will read a selection from her letters

Christopher Hollings: christopher.hollings@maths.ox.ac.uk

and unpublished manuscripts, to see what she was able to do with the powerful new modular arithmetic that had been introduced by Gauss at the beginning of the century.

The final author whom we will study in detail, Ernst Eduard Kummer (1810–1893), was also trying to develop a general method for tackling Fermat's Last Theorem, as an off-shoot of his work in what we now term *algebraic number theory*. In particular, Kummer, writing in the 1840s, noted the role that factorisation had played in several prior attempts to prove the Last Theorem. Indeed, for odd exponents, we can always write

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \cdots + y^{n-1}),$$

but as n gets larger, the right-hand factor becomes harder to deal with. Gabriel Lamé had suggested therefore that the sensible next step would be to break this down further into linear factors involving complex roots. Following through on this suggestion leads naturally to expressions involving the so-called *cyclotomic integers*: numbers of the form $a_0+a_1\omega+a_2\omega^2+\cdots+a_{n-1}\omega^{n-1}$, where $\omega = e^{2\pi i/n}$ and $a_i \in \mathbb{Z}$. A difficulty arises, however, from Kummer's surprise observation that properties of unique factorisation that we might hope to be able to carry across from the ordinary integers to their cyclotomic counterparts do not in fact hold. His solution was to develop a theory of *ideal factors* (essentially, new elements that are adjoined to the number system in question) that can be used to 'restore' unique factorisation where it is lacking. Kummer's ideal factors were later reformulated by Richard Dedekind as the *ideals* that you will have met if you took the Rings and Modules course at Part A (but you do not need to know the content of that course here). Our final piece of reading will be Kummer's introduction to his theory of ideal factors. Using this theory, Kummer went on to prove Fermat's Last Theorem for so-called *regular* prime exponents (the definition of which is beyond the scope of the present reading course).

Throughout this reading course, our interest will not merely be in the proofs of specific cases of Fermat's Last Theorem. We will use the theorem as a means of studying the emergence of wider ideas and trends in mathematics. We will see how a problem with traditional Euclidean origins helped to spark a whole new branch of mathematics, namely number theory. Beginning as an unfashionable pursuit, this gained respectability towards the end of the 18th century, and by the middle of the 19th, Fermat's Last Theorem had become one of its great unsolved problems. Mathematicians may have had to wait until the 1990s for a proof of the theorem, but even the unsuccessful attempts to prove it inspired new mathematics along the way.

Vacation reading

As preparation for the reading course, please review the MT material on the history of number theory, and revisit the relevant sections of Katz. If you have access to it, you might also like to read Simon Singh's *Fermat's Last Theorem: The story of a riddle that confounded the world's greatest minds for 358 years* (first published 1997, various editions since then). In addition, please do some biographical reading on (at least) the main figures mentioned above: Euclid, Diophantus, Fermat, Euler, Germain, Kummer. Try to make a judgement on which are the reliable biographical sources, and we will discuss these in the first class of HT.

Exercise 1

The details of some of the main texts that we will use during the reading course are given below (additional sources, both primary and secondary, will be recommended in HT). Ahead of our first class, please make sure that you have access to them—most are available online via SOLO, but you will need to turn to the Internet Archive for some of them (in particular, the Smith and Calinger sourcebooks). You will also find The Euler Archive useful: `https://scholarlycommons.pacific.edu/euler/`. If you have any difficulties, please let me know.

- Thomas Little Heath, *The thirteen books of Euclid's* Elements, 3 vols., Cambridge University Press, 1908 (this is the first edition—there have been multiple new editions and reprintings over the years, and any of these will serve for this reading course).

- Proclus, *A commentary on the first book of Euclid's* Elements, tr. Glenn R. Morrow, Princeton University Press, 2020.

- Diophantus, *Arithmetica* (3rd century CE); the recommended edition is: Jean Christianidis and Jeffrey Oaks (eds.), *The* Arithmetica *of Diophantus: A complete translation and commentary*, Routledge, 2023; we will also find it useful to look at the extracts contained in: Victor J. Katz and Clemency Montelle (eds.), *Sourcebook in the mathematics of ancient Greece and the Eastern Mediterranean*, Princeton University Press, 2024.

- Letter from Fermat to Mersenne, October 1640; published in Pierre de Fermat, *Varia opera mathematica*, Toulouse, 1679, pp. 176–178; English translation of the relevant passage (p. 177) available in Jacqueline A. Stedall, *Mathematics emerging: A sourcebook 1540–1900*, Oxford University Press, 2008, §6.1.3.

- Letter from Fermat to Frénicle, 18 October 1640; published in Pierre de Fermat, *Varia opera mathematica*, Toulouse, 1679, pp. 162–164; English translation of the relevant passage (p. 163) available in Ronald Calinger, *Classics of mathematics*, Prentice-Hall, 1995, §64.[2]

- Fermat's challenge to fellow mathematicians to solve 'Pell's equation', communicated to various recipients in early 1657, and found, for example, in

  - Pierre de Fermat, *Varia opera mathematica*, Toulouse, 1679, p. 190;

[2] NB. The translation gives an incorrect date of 10 October 1640.

Christopher Hollings: christopher.hollings@maths.ox.ac.uk

  - letter from Fermat to Frénicle, February 1657, published in Pierre de Fermat, *OEuvres de Fermat*, 4 vols., Paris: Gauthier-Villars et fils, 1891–1912, vol. II, letter LXXX.

  English translations of each of these last two items may be found in Ronald Calinger, *Classics of mathematics*, Prentice-Hall, 1995, §65.

- Fermat's observations on a remark of Bachet concerning Problem 26 of Book 2 of Diophantus's *Arithmetica*, originally published in Latin in *Diophanti Alexandrini Arithmeticorum libri sex, et De numeris multangulis liber vnus: cum commentariis C. G. Bacheti* [...] *& obseruationibus D. P de Fermat* [...] *Accessit Doctrinae analyticae inuentum nouum, collectum ex varijs eiusdem D. de Fermat epistolis* (Samuel de Fermat, ed.), Toulouse, 1670, pp. 338–339; French translation in *Œuvres de Pierre Fermat*, vol. I: *La théorie des nombres* (R. Rashed, Ch. Ouzel, and G. Christol, eds.), Paris: Librairie scientifique et technique Albert Blanchard, 1999, pp. 153–154; English translation in Jeremy Gray, *A history of abstract algebra*, Springer, 2018, p. 17.

- Leonhard Euler, 'Theorematum quorundam arithmeticorum demonstrationes', *Commentarii academiae scientiarum Petropolitanae* 10 (1747), 125–146; also published in *Opera Omnia*, series 1, vol. 2, pp. 38–58; Eneström number 98; English translation available on The Euler Archive.

- Leonhard Euler, *Vollständige Anleitung zur Algebra*, St Petersburg, 1770; recommended English translation: John Hewlett (ed.), *Elements of algebra*, 3rd ed., London, 1822.

- E. E. Kummer, 'Zur Theorie der complexen Zahlen', *Journal für reine und angewandte Mathematik* 35 (1847), 319–326; *Collected papers* (André Weil, ed.), 2 vols., Springer, 1975, vol. 1, pp. 319–326; English translation available in David Eugene Smith's *A source book in mathematics* (first published 1929, various other editions and printings since then) and also in Ronald Calinger, *Classics of mathematics*, Prentice-Hall, 1995, §109.

Exercise 2

Write a *deliberately bad* 500-word essay on any topic relating to the vacation reading. Ahead of the first class of HT, swap essays with someone else and critique each other's work. In the first class in HT, we will consider what makes a bad essay.

Christopher Hollings: christopher.hollings@maths.ox.ac.uk