BO1.1. History of Mathematics

Sheet 1 — HT26

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

Reading and Essays

Under the headings below, I set out the reading required as preparation for the classes each week. There will be three essays to complete during the term, to be handed in on the **Mondays of weeks 3, 5, and 7**: please see the further details below. Besides those sources listed week-by-week, some other items that you might find useful for general reference are:

- Oystein Ore, *Number theory and its history*, McGraw-Hill, 1948;
- John J. Watkins, *Number theory: A historical approach*, Princeton University Press, 2014;
- André Weil, *Number theory: An approach through history from Hammurapi to Legendre*, Birkhäuser, 1984.

Other general (but quite advanced) sources are:

- Harold M. Edwards, *Fermat's last theorem: A genetic introduction to algebraic number theory*, Springer, 1977;
- Paulo Ribenboim, *13 lectures on Fermat's last theorem*, Springer, 1979.

This document has three appendices. The first (A) contains a reminder of certain ideas connected with congruences that it will be useful to recall in particular when reading the work of Sophie Germain in week 6. Appendix B roughly outlines some aspects of algebraic number theory that should be useful for understanding the writings and motivation of E. E. Kummer in week 7. The final appendix (C) briefly discusses the 20th-century work on Fermat's Last Theorem that led to Andrew Wiles's proof.

Details of the assessed extended essay will be sent to you on Monday of week 7. We will devote a little time in the class in week 7 to discussion of this. In week 8, no reading is assigned: our final class will deal entirely with the extended essay.

Week 1: Preliminaries (biographies and bad essays)

Please see the Christmas Vacation Reading sheet.

Week 2: Pythagoras and Euclid

Main reading

We begin the reading course proper by looking at a concept with ancient roots, Pythagorean triples, that probably inspired some of the questions that Diophantus would later ask. Proclus,

writing in 5th century CE Athens, where he produced a commentary on the first book of Euclid's *Elements*, attributed early studies of Pythagorean triples to Pythagoras and Plato. Please read the following, which forms part of Proclus's commentary on Pythagoras's Theorem (*Elements*, Book 1, Proposition 47), and figure out what Proclus ascribed to each of the latter pair:

- Proclus, *A commentary on the first book of Euclid's* Elements, tr. Glenn R. Morrow, Princeton University Press, 2020, pp. 339–340.

The first complete classification of Pythagorean triples was that given by Euclid—please read his treatment of them:[1]

- Thomas Little Heath, *The thirteen books of Euclid's* Elements, 3 vols., Cambridge University Press, 1908 (or the edition of your choice), Book 10, Lemma 1 (preceding Proposition 29).

While we're thinking about Euclid, we'll also have a detailed look at some parts of his number-theoretic books (7–9), in preparation for Fermat's mathematics. For a general introduction to the content of these books, please read the extracts presented in:

- Victor J. Katz and Clemency Montelle (eds.), *Sourcebook in the mathematics of ancient Greece and the Eastern Mediterranean*, Princeton University Press, 2024, §2.1.

Please pay particular attention to Book 7, Definition 22 and Book 9, Proposition 36; you may find it useful to consult Heath's edition of the *Elements* for his commentaries on these parts of the text.

Other useful sources

- Jacqueline A. Stedall, *Mathematics emerging: A sourcebook 1540–1900*, Oxford University Press, 2008, §6.1.1.

The study of Pythagorean triples goes back much earlier than Pythagoras, and has been of interest beyond Europe. If you're curious, you might like to have a look at the following:

- Victor J. Katz (ed.), *The mathematics of Egypt, Mesopotamia, China, India, and Islam: A sourcebook*, Princeton University Press, 2007,

[1] You will need to know what Euclid meant by *similar plane numbers*. A *plane number* is the product of two numbers that are conceived as the sides of a rectangle; a plane number may then be thought of as an area. Two plane numbers are *similar* if the lengths of their sides are proportional in the same ratio. For example, a rectangle of size 2×4 and one of size 3×6 give rise to similar plane numbers.

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

  - p. 151, concerning Plimpton 322, an Old Babylonian clay tablet, dating from c. 1800 BCE, containing a list of Pythagorean triples;
  - pp. 458–459, featuring methods for producing Pythagorean triples from the *Līlāvatī* of Bhāskara II, a 12th-century Indian mathematical treatise.

Further material on Pythagorean triples and perfect numbers can be found in the Ore, Watkins, and Weil books cited above. On perfect numbers, see also:

- Leonard Eugene Dickson, *History of the theory of numbers*, 3 vols., New York: Chelsea Publishing Company, 1919–1923, vol. 1, ch. 1.

Week 3: Diophantus

Main reading

This week, we will look at the other strand of ancient mathematics that inspired Fermat in his number-theoretic investigations: the problems considered by Diophantus of Alexandria in the 3rd century CE, as set down in his *Arithmetica*. As an introduction to Diophantus, please read the following, at least to the end of the material on Book 2 (top of p. 90):

- Victor J. Katz and Clemency Montelle (eds.), *Sourcebook in the mathematics of ancient Greece and the Eastern Mediterranean*, Princeton University Press, 2024, §2.6.

We will then dive more deeply into the content of Book 2 of the *Arithmetica*—please read:

- Jean Christianidis and Jeffrey Oaks (eds.), *The* Arithmetica *of Diophantus: A complete translation and commentary*, Routledge, 2023, pp. 300–314.

You may also find it useful to browse some of the extensive commentary found in this volume.

Other useful sources

- Thomas L. Heath, *Diophantus of Alexandria: A study in the history of Greek algebra*, Cambridge University Press, 1910.
- Norbert Schappacher, *Diophantus of Alexandria: A text and its history*, `https://irma.math.unistra.fr/~schappa/NSch/Publications_files/1998cBis_Dioph.pdf` (accessed 25 September 2025).

Essay

What did number theory look like in the ancient world (insofar as this is reflected in the texts that you have read)? Is it anachronistic to use the term in this context, or can it be justified? (2,000 words, to be handed in by 12 noon on Monday of week 3)

Week 4: Fermat

In addition to the small part of Fermat's work that relates directly to the Last Theorem, we will also read parts of his number-theoretic writings in order to get a flavour of his wider investigations.

Main reading

- 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] a full translation of the letter may be found on The Euler Archive, attached to Euler's paper E54.

- 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;
  - letter from Fermat to Frénicle, February 1657, published in Pierre de Fermat, *Œuvres 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,

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

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

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.

In connection with the last of the above readings, it is also instructive to read what Fermat said about his method in a letter to Pierre de Carcavi of August 1659:[3]

> [1] For a long time I was unable to apply my method to affirmative questions, because the twists and turns to get there are much more difficult than those which served me for negative questions. So much so that when it occurred to me to prove that every prime number which is one more than a multiple of 4 is a sum of two squares, I found myself in a good deal of trouble. But finally a line of thought gone over many times showed me a light which did not fail, and affirmative questions surrendered to my method, with the help of some new principles which had to be joined with it of necessity. The progress in my thinking on these affirmative questions is this: if a prime number taken at one's discretion, which exceeds by one a multiple of four, is not a sum of two squares, there will be a prime number of the same kind, less than the given one, and then a third still less etc., descending infinitely this way until you arrive at the number 5 which is the smallest of all those of this kind, which it follows cannot be the sum of two squares, which it is nonetheless. From which one must infer from that deduction of an impossibility that all those of this kind are consequently a sum of two squares.
>
> [2] There are infinitely many questions of this kind, but there are some others which demand new principles before the descent can be applied to them and the study of them is sometimes so difficult one cannot overcome without extreme effort. Such is the following question that Bachet said Diophantus had never been able to demonstrate, on the subject of which M. Descartes in one of his letters made the same declaration when he confessed that he found it so difficult that he could see no way of solving it.
>
> Every number is a square, or a sum of two, three, or four squares.
>
> I have finally organized this according to my method and shown that if a given number is not of this nature there will be a smaller which is also not, then a third less than the second, etc., to infinity, from which one infers that all numbers are of this nature.
>
> [3] What I proposed to M. Frenicle and others is also of this great or even greater difficulty: Every non-square number is of such a nature that there are infinitely many squares which, multiplying the said number are one less than a square. I proved it by a descent applied in a quite particular manner.

[3] Published in Pierre de Fermat, *Œuvres de Fermat*, 4 vols., Paris: Gauthier-Villars et fils, 1891–1912, vol. II, letter CI; the English translation which we quote here is taken from John Fauvel and Jeremy Gray, *The history of mathematics: A reader*, Macmillan, 1987, §11.C7.

I admit that M. Frenicle gave various particular solutions and M. Wallis also, but the general proof is found by a descent strictly and properly applied, which I will show them so that they can add the proof and general construction of the theorem and of the problem to the singular solutions which they gave.

[4] Finally I considered certain questions which, although negative, did not shrink from receiving very great difficulties, the way of applying the descent being quite as diverse as the preceding, as it will be easy to check. These are the following:

No cube is a sum of two cubes.

There is only one square in integers which, added to two, gives a cube. The said square is 25.

There are only two squares in integers which, added to 4, give a cube. The said squares are 4 and 121.

All the square powers of two, added to one, are prime numbers.

This last question is of a very subtle and ingenious study and, even though it is posed affirmatively, it is negative; for to say that a number is prime is to say that it cannot be divided by any number.

I put in this place the following question of which I have sent the proof to M. Frenicle after he told me and even showed me in his printed writings that he could not find it.

There are only the two numbers 1 and 7 which, being less by 1 than the double of a square make squares of the same kind, that is to say which are less by one than the double of a square.

Other useful sources

- Harold M. Edwards, *Fermat's last theorem: A genetic introduction to algebraic number theory*, Springer, 1977, ch. 1.
- Michael S. Mahoney, *The mathematical career of Pierre de Fermat (1601–1665)*, Princeton University Press, 1973; 2nd ed., 1994.
- Paulo Ribenboim, *13 lectures on Fermat's last theorem*, Springer, 1979, lecture I, §1.
- Jacqueline A. Stedall, *Mathematics emerging: A sourcebook 1540–1900*, Oxford University Press, 2008, §§6.1.2, 6.2, 6.3.

Exercise 1

To prove that Fermat's equation $x^n + y^n = z^n$ has no integer solutions for $n > 2$, why does it suffice to show this only for $n = 4$ and for odd prime exponents p?

Exercise 2

In the period between Fermat's marginal note and Andrew Wiles's proof, what did people think of Fermat's claim to have proved his Last Theorem? Gather as many examples as you can, for discussion in the class.[4]

Week 5: Euler

Main reading

- 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.
  - NB. The material from Theorem 2 onwards is less important for our purposes—do please read it, but it is not necessary to understand every detail.
- Leonhard Euler, *Vollständige Anleitung zur Algebra*, St Petersburg, 1770; recommended English translation: John Hewlett (ed.), *Elements of algebra*, 3rd ed., London, 1822. Please read Part II, Chapter XIII, 'Of some Expressions of the Form $ax^4 + by^4$, which are not reducible to Squares' (pp. 405–413).

Also relevant here is the following extract from a letter that Euler wrote to Christian Goldbach in August 1753:[5]

> There's another very lovely theorem in Fermat whose proof he says he has found. Namely, on being prompted by the problem in Diophantus, find two squares whose sum is a square, he says that it is impossible to find two cubes whose sum is a cube, and two fourth powers whose sum is a fourth power, and more generally that this formula $a^n + b^n = c^n$ is impossible when $n > 2$. Now I have found valid proofs that $a^3 + b^3 \neq c^3$ and $a^4 + b^4 \neq c^4$, where $\neq$ denotes cannot equal. But the proofs in the two cases are so different from one another that I do not see any possibility of deriving a general proof from them that $a^n + b^n \neq c^n$ if $n > 2$. Yet one sees quite clearly as if through a trellis that the larger n is, the more impossible the formula must be. Meanwhile I haven't yet been able to prove that the sum of two fifth powers cannot be a fifth power. To all appearances the proof just depends on a brainwave, and until one has it all one's thinking might as well

[4] No need to hand in anything for either of these exercises.

[5] Published in P. H. Fuss, *Correspondance mathématique et physique de quelques célèbres géomètres du XVIII-ème siècle*, 2 vols., St Petersburg, 1843, vol. I, letter CLV; the English translation which we quote here is taken from John Fauvel and Jeremy Gray, *The history of mathematics: A reader*, Macmillan, 1987, §14.C2(a).

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

> be in vain. But since the equation $aa + bb = cc$ is possible, and so also is this possible, $a^3 + b^3 + c^3 = d^3$, it seems to follow that this, $a^4 + b^4 + c^4 + d^4 = e^4$, is possible, but up till now I have been able to find no case of it. But there can be five specified fourth powers whose sum is a fourth power.

Finally, you might like to browse the following papers to get a sense of how Euler's number-theoretic investigations related to those of Fermat:

- Leonhard Euler, 'Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus', *Commentarii academiae scientiarum Petropolitanae* 6 (1738), pp. 103–107; also published in *Opera Omnia*, series 1, vol. 2, pp. 1–5; Eneström number 26; English translation available on The Euler Archive.
- Leonhard Euler, 'Theorematum quorundam ad numeros primos spectantium demonstratio', *Commentarii academiae scientiarum Petropolitanae* 8 (1741), 141–146; also published in *Opera Omnia*, series 1, vol. 2, pp. 33–37; Eneström number 54; English translation available on The Euler Archive.

Other useful sources

- Harold M. Edwards, *Fermat's last theorem: A genetic introduction to algebraic number theory*, Springer, 1977, §§2.1–2.2.
- Jeremy Gray, *A history of abstract algebra*, Springer, 2018, §2.3.
- Paulo Ribenboim, *13 lectures on Fermat's last theorem*, Springer, 1979, lecture I, §2.
- C. Edward Sandifer, *The early mathematics of Leonhard Euler*, MAA, 2007.

Essay

Discuss the place of Fermat's number-theoretic investigations within the wider mathematical landscape of 17th-century Europe. How and to whom did he communicate his ideas, and what did his readers make of them?

(2,000 words, to be handed in by 12 noon on Monday of week 5)

Week 6: Germain

Little of Sophie Germain's number-theoretic work was published during her lifetime. In particular, her research connected with Fermat's Last Theorem exists only in the form of unpublished manuscripts and in some of her correspondence. Fortunately for us, these have been published, though mostly only in the original French.

Main reading

- Letter from Sophie Germain to Carl Friedrich Gauss, 12 May 1819; this can be found in French in 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); an English translation is available on the course webpage.

The bulk of Germain's further research on Fermat's Last Theorem is contained in a series of unpublished and undated French manuscripts held in the Bibliothèque Nationale de France and the Biblioteca Moreniana in Florence. A full transcription of one of the Florentine manuscripts ('Remarque sur l'impossibilité de satisfaire en nombres entiers a l'équation $x^p + y^p = z^p$') can be found as an appendix to Andrea Del Centina, 'Unpublished manuscripts of Sophie Germain and a revaluation of her work on Fermat's Last Theorem', *Archive for History of Exact Sciences* 62 (2008), 349–392. Because Germain's writing is quite dense, we confine our attention here to a short extract from one of the Parisian manuscripts ('Démonstration de l'impossibilité de satisfaire en nombres entiers à l'équation $z^{2(8n\pm3)} = y^{2(8n\pm3)} + x^{2(8n\pm3)}$'), as translated by Reinhard Laubenbacher and David Pengelley (*Mathematical expeditions: Chronicles by the explorers*, Springer, 1999, pp. 190–191):

> First Theorem. For any [odd] prime number p in the equation $z^p = x^p + y^p$ one of the three numbers z, x, or y will be a multiple of p^2.
>
> To prove this theorem it suffices to suppose that there exists at least one prime number θ of the form $2Np + 1$ for which at the same time one cannot find two pth power residues whose difference is one, and p is not a pth power residue. Not only does there always exist a number θ satisfying these two conditions, but the course of calculation indicates that there must be an infinite number of them. For example, if $p = 5$, then $\theta = 2 \cdot 5 + 1 = 11,\ 2 \cdot 4 \cdot 5 + 1 = 41,\ 2 \cdot 7 \cdot 5 + 1 = 71,\ 2 \cdot 10 \cdot 5 + 1 = 101,$ etc.
>
> Let therefore $z = lr,\ x = hn,\ y = vm$. If one assumes that p is [relatively] prime to $z, x,$ and y, then one will have that
>
> $$\begin{aligned} x + y &= l^p, & x^{p-1} - x^{p-2}y + x^{p-3}y^2 - x^{p-4}y^3 + \text{etc} &= r^p, \\ z - y &= h^p, & z^{p-1} + z^{p-2}y + z^{p-3}y^2 + z^{p-4}y^3 + \text{etc} &= n^p, \\ z - x &= v^p, & z^{p-1} + z^{p-2}x + z^{p-3}x^2 + z^{p-4}x^3 + \text{etc} &= m^p. \end{aligned}$$
>
> Since we have assumed that there are no two pth power residues modulo θ whose difference is one, it follows that in the equation $z^p = x^p + y^p$ one of the numbers x, y, z is necessarily a multiple of θ. To make a choice, let us take $z \equiv 0 \pmod{\theta}$. Thus one has $l^p + h^p + v^p \equiv 0 \pmod{\theta}$. It is therefore necessary, again, that one of the numbers l, h, v be a multiple of θ; because $z = lr \equiv 0$ it can only be l. And as a result $x \equiv -v^p,\ y \equiv -h^p,\ x + y \equiv 0 \pmod{\theta}$. Consequently $px^{p-1} \equiv pv^{p(p-1)} \equiv r^p$. That is to say, p is a pth power residue, contrary to the hypothesis.

Can you make sense of Germain's argument? What is she trying to demonstrate? Is the proof complete? How does it relate to Fermat's Last Theorem?

Other useful sources

- Andrea Del Centina and Alessandra Fiocca, 'On the Correspondence of Sophie Germain', in *Mathematical correspondences and critical editions* (Maria Teresa Borgato, Erwin Neuenschwander and Irène Passeron, eds.), Birkhäuser, 2018, pp. 147–166.
- Harold M. Edwards, *Fermat's last theorem: A genetic introduction to algebraic number theory*, Springer, 1977, §3.2.
- Reinhard Laubenbacher and 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.
- Dora Musielak, *Sophie Germain: Revolutionary mathematician*, 2nd ed., Springer, 2020.
- Paulo Ribenboim, *13 lectures on Fermat's last theorem*, Springer, 1979, lecture IV, §2.

Essay

In March 1816, Gauss wrote the following to the astronomer Wilhelm Olbers:[6]

> I do admit that the Fermat Theorem as an isolated result is of little interest to me, since it is easy to postulate a lot of such theorems, which one can neither prove nor refute. Nonetheless, it has caused me to return to some old ideas for a *great* extension of higher arithmetic [number theory]. Of course, this theory is one of those things where one cannot presuppose to what extent one will succeed in reaching goals looming in the far distance. A lucky star must also preside, and my situation as well as much detracting business do not allow me to indulge in such meditations as during the lucky years 1796–1798, when I formed the main parts of my Disquisitiones Arithmeticae. Alas, I am convinced, that if *luck* contributes more than I am allowed to hope for, and I succeed in some of the main steps in that theory, then the Fermat theorem will appear in it as one of the least interesting corollaries.

What do you make of Gauss's opinion of Fermat's Last Theorem? Why might Gauss have found the result uninteresting? To what extent were Gauss's views reflective of those of his contemporaries?

(2,000 words, to be handed in by 12 noon on Monday of week 7)

[6] Published in C. Schilling (ed.), *Wilhelm Olbers: Sein Leben und seine Werke. Zweiter Band: Briefwechsel zwischen Olbers und Gauss. Erste Abtheilung*, Berlin: Spinger, 1900, letter no. 321; the English translation which we quote here is taken from Reinhard Laubenbacher and David Pengelley, *Mathematical expeditions: Chronicles by the explorers*, Springer, 1999, p. 167.

Week 7: Kummer

Among the various proofs for specific exponents that came after Germain's attempt at a more general approach to Fermat's Last Theorem, the French mathematician Gabriel Lamé surprised the Paris Academy by announcing a proof of the theorem in 1847. Although the subsequent arguments that took place at the Academy showed Lamé's proof to be wrong, he introduced an approach that was to prove fruitful later on. Given that we may confine our attention to odd prime exponents in Fermat's equation, we may always write down the factorisation

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

But as Lamé observed, as we consider larger n, the degree of the right-hand factor grows, and it becomes increasingly unwieldy. His proposal, therefore, was to step outside the integers, and factor the right-hand side of (1) into linear factors using complex numbers. Let ω be the primitive n-th root of unity, i.e., $\omega = e^{2\pi i/n}$. Then (1) can be rewritten:

$$x^n + y^n = (x + y)(x + \omega y)(x + \omega^2 y) \cdots (x + \omega^{n-1} y). \tag{2}$$

Like others before him, Lamé sought to employ an infinite descent argument: if the right-hand side of (2) is equal to an n-th power, namely z^n, and the linear factors can be shown to be pairwise coprime in an appropriate sense, then it would follow that each factor is itself an n-th power, smaller than z^n, and so on. The problem with this method, and the cause of the arguments at the Academy, is that it assumes that ideas about unique prime factorisation may be carried across from the positive integers into other number systems, such as the special subset of the complex numbers, 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 $a_i \in \mathbb{Z}$), that is needed here. That this was not the case was shown by the German mathematician Ernst Eduard Kummer, who also proposed a way to remedy the situation. (Since the cyclotomic integers are difficult to work with, an outline of Kummer's ideas in the context of the friendlier number system $\mathbb{Z}[\sqrt{-5}]$ is given in Appendix B.)

Main reading

- 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.
- 'Extrait d'une lettre de M. Kummer à M. Liouville', *Journal de mathématiques pures et appliquées* 12 (1847), 136; *Collected papers* (André Weil, ed.), 2 vols., Springer, 1975, vol. 1, p. 298; an English translation is available on the course webpage.

By way of rounding off this reading, we note that Kummer was able subsequently (1850) to use his method of ideal numbers to 'restore' unique factorisation, and thus prove Fermat's Last Theorem by infinite descent, in the case of so-called *regular* primes (the definition of these is, however, outside the scope of the present reading course).

Other useful sources

- Harold M. Edwards, *Fermat's last theorem: A genetic introduction to algebraic number theory*, Springer, 1977, §4.1.
- John Fauvel and Jeremy Gray, *The history of mathematics: A reader*, Macmillan, 1987, §15.C2.
- Jeremy Gray, *A history of abstract algebra*, Springer, 2018, ch. 16.
- Paulo Ribenboim, *13 lectures on Fermat's last theorem*, Springer, 1979, lecture I, §3; lecture V.

Week 8: General discussion

No reading is assigned for this week. Instead, we will use the class to discuss the extended essay, and to return to any topics that you would find it useful to consider further—do please come along with suggestions, or email me in advance.

Appendix A: A reminder about congruences

The language of modular arithmetic was introduced by Gauss in his *Disquisitiones arithmeticae* of 1801 to streamline mathematical discussions involving the divisibility of integers. In this term's reading, we will see Euler making arguments in this area in a largely verbal form prior to the introduction of Gauss's new notation, and later on we will see Germain writing out her ideas about Fermat's Last Theorem in this new language. You are probably familiar with the basic language of modular arithmetic (those who took the Part A short option Number Theory will have had more recent practice in it), but this appendix is offered as a brief reminder of the key ideas.

For $a, b, m \in \mathbb{Z}$, we write $a \equiv b \,(\mathrm{mod}\, m)$ to mean that $a-b$ is divisible by m, i.e., $a-b = km$, for some $k \in \mathbb{Z}$. Congruence modulo m is of course an equivalence relation, and it behaves in other nice ways:

if $a \equiv b \,(\mathrm{mod}\, m)$ and $c \equiv d \,(\mathrm{mod}\, m)$, then $a + c \equiv b + d \,(\mathrm{mod}\, m)$ and $ac \equiv bd \,(\mathrm{mod}\, m)$.

Division, on the other hand, only works in certain circumstances: in order to cancel the k from the congruence $ka \equiv kb \,(\mathrm{mod}\, m)$, we must have that k and m are *coprime* (a.k.a. *relatively prime*),[7] i.e., $\gcd(k, m) = 1$. Given any integers a, m, the Division Algorithm enables us to find positive integers q, r such that $a = qm + r$, where $0 \leq r < m$. This means that when considering congruence modulo m, we may restrict our attention to the set of *residues* $\{0, 1, 2, \ldots, m-1\}$.

We recall one of the simple applications of modular arithmetic. We can prove that no number of the form $4k + 3$ can ever be a sum of two squares by noting that any square number must be congruent either to 0 or to 1 modulo 4, since $0^2 \equiv 2^2 \equiv 0 \,(\mathrm{mod}\, 4)$ and $1^2 \equiv 3^2 \equiv 1 \,(\mathrm{mod}\, 4)$. Hence, a sum of two squares can only be congruent to 0, 1, or 2 modulo 4, QED. We will see Euler proving this result but in a much more verbal manner.

In our reading of Fermat, we will see him communicating to Frénicle the result that is now known as Fermat's Little Theorem. Although this language was not available to Fermat, it is usually phrased nowadays in terms of modular arithmetic: if p is prime and a is an integer, then $a^p \equiv a \,(\mathrm{mod}\, p)$. Alternatively, if we add the condition that a not be divisible by p, then the statement of the theorem becomes $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$.

Finally, we need to know what is meant by the term *power residue*, which comes up in Germain's writing. A subject of great interest to Gauss and others in the late-18th and early-19th centuries was *reciprocity laws*. The simplest case of these relates to *quadratic residues* (Germain sometimes called them *square residues*): an integer a is a *quadratic residue modulo* p if it is congruent to a square modulo p, i.e., if there exists b such that $a \equiv b^2 \,(\mathrm{mod}\, p)$. The study of quadratic residues has relevance for the solution of quadratic congruences of the form $ax^2 + bx + c \equiv 0 \,(\mathrm{mod}\, p)$, where p is usually prime. The *law of quadratic reciprocity* (whose statement we omit), first proved by Gauss, provides an easy way to determine whether a given integer is a quadratic residue for a particular modulus. Its utility led subsequently to the search for *higher reciprocity laws*: methods for determining whether a given integer is a cubic residue, a quartic residue, and so on, where each of these concepts is defined via a natural adaptation of the notion of a quadratic residue. Germain made extensive use of *p-th power residues*: an integer a is a *p-th power residue modulo* p if there exists b such that $a \equiv b^p \,(\mathrm{mod}\, p)$.

Appendix B: Some relevant algebraic number theory

These notes are intended as rough mathematical background to the ideas that we will see in our reading of Kummer's work.[8] Some of the ideas will be familiar to those who took the Rings

[7] Since we've mentioned coprime numbers, we take the opportunity to note a result that is needed to understand both Germain's and Kummer's approaches to Fermat's Last Theorem: if the product of two coprime numbers is an n-th power, then each of the numbers is. This is a consequence of the Fundamental Theorem of Arithmetic.

[8] Parts of these notes are adapted from Reinhard Laubenbacher and David Pengelley, *Mathematical expeditions: Chronicles by the explorers*, Springer, 1999, §4.5.

and Modules course at Part A, **but a detailed knowledge of this area (algebraic number theory) is not necessary for this reading course**.

As we will see, the issue of unique factorisation lies at the heart of Kummer's work—in particular, the fact that the familiar Fundamental Theorem of Arithmetic on the unique factorisation of positive integers into primes does not extend automatically to other number systems. To begin to understand why, we first need to consider how we define primes. In the positive integers, we most commonly define a prime p to be a number with the following property:

$$\text{for } m \in \mathbb{N}, \text{ if } m \mid p, \text{ then either } m = 1 \text{ or } m = p. \tag{3}$$

We also like to deduce the following useful property of a prime p:

$$\text{for } m, n \in \mathbb{N}, \text{ if } p \mid mn, \text{ then } p \mid m \text{ or } p \mid n. \tag{4}$$

In fact, statements (3) and (4) are equivalent in $\mathbb{N}$, so we could take (4) as our definition of a prime if we were so inclined. Indeed, in number systems other than $\mathbb{N}$, we end up doing just that, because in other systems that are of interest, (3) and (4) are no longer equivalent (though (4) always implies (3)). We therefore reserve the word *prime* for a quantity defined by (4); quantities defined by (3) are called *irreducibles*. Beyond $\mathbb{N}$, we usually find it most appropriate to consider factorisations into irreducibles.

A useful illustrative example of these ideas is provided by the set

$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

This is closed under addition and multiplication of complex numbers, and therefore forms a number system in which we can consider the factorisation of elements (to be precise, it is an *integral domain*). We notice first of all that in $\mathbb{Z}[\sqrt{-5}]$, 6 has two different factorisations, namely:

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{5}$$

Not all of the factors involved are prime in $\mathbb{Z}[\sqrt{-5}]$, but they are all irreducible (exercise). Thus, unique factorisation (specifically, the uniqueness) fails in $\mathbb{Z}[\sqrt{-5}]$. It is something very much like this that Kummer proved in the context of the cyclotomic integers

$$\mathbb{Z}[\omega] = \{a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{n-1}\omega^{n-1} : a_i \in \mathbb{Z}\},$$

where ω is the primitive n-th root of unity. He showed that unique factorisation holds for $n \leq 19$, but fails for $n = 23$ (and all higher primes). In particular, it is possible to show in this latter case that the product

$$(1 + \omega^2 + \omega^4 + \omega^5 + \omega^6 + \omega^{10} + \omega^{11})(1 + \omega^5 + \omega^6 + \omega^7 + \omega^9 + \omega^{11})$$

is divisible by 2 (which is irreducible), but 2 divides neither factor.

As Kummer observed, uniqueness of factorisation had been key to some prior approaches to the proof of Fermat's Last Theorem for small exponents, but it fails when the exponent grows too large. He therefore sought a means of 'restoring' unique factorisation where it was lacking, and he did this through the device of *ideal numbers*.

To illustrate the principle behind Kummer's ideal numbers, let us consider the set

$$X = \{a \in \mathbb{N} : a \equiv 1 \pmod 5\}.$$

This is clearly closed under multiplication, so we can talk about factorisation of its elements. Notice that 6 is irreducible in X, but not prime, since $6 \times 56 = 336 = 16 \times 21$ and neither 16 nor 21 is divisible by 6. But 16, 21, and 56 are all irreducible, so the factorisation of 336 into irreducibles in X is not unique. The reason for this breakdown in unique factorisation is our slightly artificial restriction to X. We know that in the wider setting of the positive integers, 6 is *not* irreducible, since it factorises as 2×3, but while we are confining our attention to X, the factors 2 and 3 are inaccessible to us. The principle behind Kummer's ideal numbers is the implicit extension of our number system in such a way that we include new numbers that will serve as irreducible factors and thereby 'restore' unique factorisation. In our earlier example (5) in $\mathbb{Z}[\sqrt{-5}]$, we might, for example, assert the existence a new (ideal) common divisor of 2 and $1 + \sqrt{-5}$.

In their original formulation, Kummer's ideal numbers are rather slippery concepts, since they are never quite written down explicitly. Instead, they are studied in terms of how they interact with the elements of our number system. In particular, we are interested in seeing which numbers they divide. This can be illustrated by returning to our example of $\mathbb{Z}[\sqrt{-5}]$ and following the thread established at the end of the previous paragraph: we consider the ideal common divisor of a pair of elements by analogy with the greatest common divisor in $\mathbb{N}$. In $\mathbb{N}$, the greatest common divisor of a pair of numbers necessarily divides all linear combinations of those numbers, and conversely, the set of all such linear combinations determines the greatest common divisor uniquely. We can apply a similar idea in the case of ideal common divisors in $\mathbb{Z}[\sqrt{-5}]$, by representing the ideal common divisor of two numbers via the set of all linear combinations of those two numbers over $\mathbb{Z}[\sqrt{-5}]$. Thus, if we denote by A the ideal common divisor of 2 and $1 + \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$, we can also consider A to be the set of all linear combinations of these numbers:

$$A = \{2m + (1 + \sqrt{-5})n : m, n \in \mathbb{Z}[\sqrt{-5}]\}.$$

(Here we see one of the confusing aspects of handling ideal numbers: we are considering A simultaneously as a number and a set.) Now that we have this representation of ideal numbers in terms of linear combinations, we see also that it need not only apply to pairs of numbers:

$$\{2k : k \in \mathbb{Z}[\sqrt{-5}]\},$$

for instance, is a perfectly valid ideal number—the ideal number of all elements that are divisible by 2 in $\mathbb{Z}[\sqrt{-5}]$.

The use of linear combinations enables us to do arithmetic with ideal numbers. Suppose, for example, that we want to compute A^2. (Set multiplication is understood here as $S^2 = SS = \{ab : a, b \in S\}$.) Since $2^2 = 4$ and $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5}$, we have in the first instance that

$$A^2 = \{4k + 2(1+\sqrt{-5})m + (-4+2\sqrt{-5})n : k, m, n \in \mathbb{Z}[\sqrt{-5}]\}.$$

So every element of A^2 is divisible by 2. But notice further that since $4, -4+2\sqrt{-5} \in A^2$, we also have $4+(-4+2\sqrt{-5}) = 2\sqrt{-5} \in A^2$, from which it follows that $2(1+\sqrt{-5})-2\sqrt{-5} = 2 \in A^2$. This upshot of all this is that in fact

$$A^2 = \{2k : k \in \mathbb{Z}[\sqrt{-5}]\}.$$

Now let B be the ideal common divisor of 3 and $1+\sqrt{-5}$, and C be the ideal common divisor of 3 and $1-\sqrt{-5}$. Applying simliar reasoning to that above, we can calculate

$$\begin{aligned} AB &= \{(1+\sqrt{-5})k : k \in \mathbb{Z}[\sqrt{-5}]\}, \\ BC &= \{3k : k \in \mathbb{Z}[\sqrt{-5}]\}, \\ AC &= \{(1-\sqrt{-5})k : k \in \mathbb{Z}[\sqrt{-5}]\}. \end{aligned}$$

Hence, AB, BC, and AC are, respectively, the ideal numbers of all elements that are divisible by $1+\sqrt{-5}$, 3, and $1-\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$. Noting that, according to this scheme, the ideal number of all elements that are divisible by 6 in $\mathbb{Z}[\sqrt{-5}]$ may be represented as $\{6k : k \in \mathbb{Z}[\sqrt{-5}]\}$, we rewrite (5) in terms of multiplication of ideal numbers:

$$\begin{aligned} \{6k : k \in \mathbb{Z}[\sqrt{-5}]\} &= \{2k : k \in \mathbb{Z}[\sqrt{-5}]\}\{3k : k \in \mathbb{Z}[\sqrt{-5}]\} \\ &= A^2BC \\ &= ABAC \\ &= \{(1+\sqrt{-5})k : k \in \mathbb{Z}[\sqrt{-5}]\}\{(1-\sqrt{-5})k : k \in \mathbb{Z}[\sqrt{-5}]\}. \end{aligned}$$

Thus, A^2BC serves as the 'missing' factorisation of 6 (unique up to the order of the factors) in $\mathbb{Z}[\sqrt{-5}]$.

We can see from the above that Kummer's language of ideal numbers can be rather tricky to apply, and cumbersome to write down. It is for this reason that a reformulation of these ideas was subsequently proposed by Richard Dedekind: since ideal numbers can be represented via the sets of elements that they divide, we can leave aside the ideal numbers entirely, and work more simply and directly in terms of these sets. In Dedekind's version, our A from above, now denoted $\langle 2, 1+\sqrt{-5}\rangle$, becomes the *ideal* generated by 2 and $1+\sqrt{-5}$. It is closed under addition and under multiplication by elements of $\mathbb{Z}[\sqrt{-5}]$, so it forms a structure that is susceptible to

treatment in the language of abstract algebra that was taking off in the late 19th century—it is in precisely this form that you will have encountered ideals if you took the Rings and Modules course at Part A. We can easily define an arithmetic of ideals, including an appropriate notion of prime ideal, and when considering number systems that do not admit unique factorisation, we can often turn our attention instead to their systems of ideals and find that unique factorisation holds there—precisely what Kummer was doing, but in a different language.

Appendix C: A rough sketch of what happened next

In our reading, we will take the story of the proof of Fermat's Last Theorem as far as the mid-19th century. It is difficult for us to take it much further, as the mathematics involved gets considerably harder as we move into the 20th century. This appendix gives a very rough indication of where things went next.

In the early 20th century, efforts to prove Fermat's Last Theorem remained quite traditionally number-theoretic in their style. For instance, in 1909, Arthur Wieferich proved that if the equation $x^p + y^p = z^p$ has a solution for a prime p with $p \nmid xyz$, then p must satisfy the congruence $2^{p-1} \equiv 1 \,(\text{mod } p^2)$. Later in the 20th century, computer-based methods were used to tackle particular cases of the Last Theorem, but generally by implementing techniques coming from number theory.

The biggest shift in the treatment of Fermat's Last Theorem during the 20th century, however, was towards the application of techniques from algebraic geometry. Simply (or simplistically) put, algebraic geometry is the study of solution sets of polynomials in several variables. The equation $x^n + y^n = z^n$ fits into this mould very naturally, and can in fact be replaced by a slightly simpler version: instead of looking for integer solutions of $x^n + y^n = z^n$, we instead seek rational solutions of $x^n + y^n = 1$, which of course lie on a curve, the corresponding *Fermat curve*, in the Euclidean plane (for simplicity, we are tip-toeing around the fact that a Fermat curve is more properly defined in the *complex projective plane*). We can apply the geometrical notion of *genus* (intuitively: 'number of holes') to this curve in a natural way. It turns out that the Fermat curve corresponding to the equation $x^n + y^n = 1$ has genus $\frac{(n-1)(n-2)}{2}$ for $n \geq 2$, so for $n = 2$, we have a curve of genus 0 (a conic), and for $n = 3$, a curve of genus 1 (an elliptic curve). If $n \geq 4$, the genus always exceeds 1.

The starting point for the application of algebraic geometry to Fermat's Last Theorem was what used to be termed **Mordell's Conjecture**, proposed by Louis Mordell in 1922: any curve over $\mathbb{Q}$ of genus greater than 1 has only finitely many rational points (i.e., points with rational coordinates). Thus, if the curve corresponding to the equation $x^n + y^n = 1$ (with $n \geq 4$ to ensure that the curve has genus greater than 1) has only finitely many rational points, then there can be only finitely many pairwise coprime integer solutions to the equation $x^n + y^n = z^n$. The relevance of this conjecture to Fermat's Last Theorem is that it cuts down the number of

potential solutions for any $n \geq 4$ to a finite set (cf. the rephrasing of Fermat's Last Theorem in this context: that a Fermat curve has no nontrivial rational points). Mordell's Conjecture was proved by Gert Faltings in 1983, and thereafter was renamed **Faltings's Theorem**; his proof of the Mordell Conjecture was one of the results that won Faltings a Fields Medal.

As the links between algebraic geometry and number theory grew during the 20th century (giving rise to a field that is sometimes called *arithmetic geometry*), a number of conjectures were made that, if true, would imply Fermat's Last Theorem. The most important of these, as it turned out, was the **Taniyama–Shimura Conjecture** (after Yutaka Taniyama and Goro Shimura, who stated it in the 1950s), which asserts, in its short form, that all elliptic curves over $\mathbb{Q}$ are modular. To begin to unpack this, we recall that an elliptic curve over $\mathbb{Q}$ is one of the form $y^2 = Ax^3 + Bx^2 + Cx + D$, where $A, B, C, D \in \mathbb{Q}$, $A \neq 0$, and the polynomial on the right-hand side has no repeated roots. We also need to know the (slightly more involved) definition of a modular function: a function $f(z)$ defined on the upper half-plane $\{z = x + iy : y > 0\}$ is called a *modular function of level* N if it is meromorphic (recall from last year's Complex Analysis course that this means that it is holomorphic everywhere except at isolated points) and for all $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$ and $N \mid c$, we have $f(\frac{az+b}{cz+d}) = f(z)$. An elliptic curve is said to be *modular* if it can be parametrised by modular functions. Thus, the Taniyama–Shimura Conjecture can be restated as follows: for any elliptic curve $y^2 = Ax^3 + Bx^2 + Cx + D$ over $\mathbb{Q}$, there are non-constant modular functions $f(z)$, $g(z)$ of the same level such that $f(z)^2 = Ag(z)^3 + Bg(z)^2 + Cg(z) + D$.

The Taniyama–Shimura Conjecture owes its connection to Fermat's Last Theorem to some work by Gerhard Frey, published in 1986. Supposing (a, b, c) to be a nontrivial solution of the equation $x^p + y^p = z^p$ for some prime exponent $p \geq 5$, Frey constructed an associated elliptic curve $y^2 = x(x - a^p)(x + b^p)$, and claimed that this is not modular. A gap in Frey's argument was filled by Ken Ribet in 1990, thereby showing that the Taniyama–Shimura Conjecture implies Fermat's Last Theorem (think about the contrapositive in connection with Frey's idea). In fact, for this implication to work, it is enough to use the Taniyama–Shimura Conjecture in the case of a special type of elliptic curves called a *semistable* elliptic curves, and this is precisely what Andrew Wiles achieved (with some help from Richard Taylor): a proof of the Taniyama–Shimura Conjecture for semistable elliptic curves, from which Fermat's Last Theorem then follows. (By 2001, a proof of the Taniyama–Shimura Conjecture in full generality had been attained by the collective efforts of Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor; it is now known as the **Modularity Theorem**.)