FLT as a theorem whose meaning was constituted by its failures

Introduction

Along with the passing mention of a proof too large to be written down, the claim that $x^n + y^n = z^n$ has no positive integer solutions for $n > 2$ first appeared as a note in the margins of Pierre de Fermat's personal copy of Bachet's translation of Diophantus's *Arithmetica*. Published posthumously by his son, Samuel de Fermat, in the 1670 Toulouse edition (Bachet 1670, p. 61), the note survived as a provocation for three centuries. Between that note and Andrew Wiles's 1995 proof, not a single attempt to resolve Fermat's Last Theorem (FLT) proved successful. However, each serious attempt did provided a useful diagnosis of where the mathematical tools of the era fell short. Each failure exposed a new structural inadequacy in the arithmetic language used to attack it, and it was the repair of that inadequacy, rather than the attempted proof, which became the lasting mathematical contribution.

This essay argues that FLT functioned as a *diagnostic instrument*: a statement simple enough to be posed in any arithmetic framework, but rich enough in structure that it required the full mathematical machinery of the late-twentieth century to resolve. At the same time, a theorem can only diagnose what it encounters, so FLT's diagnostic power depended on its capacity to draw mathematicians toward it. Therefore, the theorem also functioned as an *occasion*: its simplicity of statement, its authorship by a brilliant amateur who—unlike the predominant role of mathematicians as systematic expositors at the time—preferred the role of analyst (Mahoney 1994, pp. 11–14), and Fermat's tantalising claim to possess a proof created an intellectual and social magnetism, all ensured FLT made repeated contact with new mathematical frameworks. Each time FLT was taken up, new tools were brought to bear, transformed by the previous attempt. Each diagnosis prompted repair, the repair created a new framework, and the new framework made

FLT legible as a different problem, drawing mathematicians back to it on altered terms. The relationship between FLT and the discipline it helped shape resembles what Goldstein and Schappacher (2007, pp. 3–5) describe for Carl Friedrich Gauss's *Disquisitiones Arithmeticae*: it generated a field even though it was not the singular static cause, and its influence depended on being reappropriated by successive communities for their own purposes.

There is a natural objection to this reading. Gauss, writing to Heinrich Olbers in March 1816, called FLT "an isolated result" of little interest. He predicted that if his project of higher arithmetic succeeds, FLT would appear "as one of the least interesting corollaries" (Gauss to Olbers, 21 March 1816, in Laubenbacher and Pengelley 1999, p. 167). Gauss was not alone in his dismissal: Ernst Kummer, as Harold Edwards reported (1977, pp. 79–80), regarded his FLT result for regular primes as "a curiosity of number theory rather than a major item," instead considering higher reciprocity to be the discipline's central problem. This view that FLT was an isolated theorem that merely spectated the evolution of modern mathematics—until Wiles's proof coincidentally resolved it—offers a counterpoint to the thesis of this essay: that FLT measured, convened, and thereby helped animate the development of new mathematical machinery.

The four case studies below—covering attempts by Fermat, Leonard Euler, Sophie Germain, and Kummer—push back against that isolationist view. Even where FLT was not the primary motivation for new mathematics, its emergence as a social and mathematical object of fascination exposed novel inadequacies. Indeed, across these case studies, FLT exhibited a progression of failure modes that can be classified as failure of *method*, failure of *assumption*, failure of *reach*, and failure of *generality*. "Method" names Fermat's case because infinite descent worked for $n = 4$ but offered no mechanism for scaling. "Assumption" names Euler's because a structural property was imported into a new domain without being recognised as requiring justification. "Reach" names Germain's because her reasoning was sound and her assumptions correct, but the distributional result she required about primes lay beyond what elementary congruence arguments could deliver. "Generality" names Kummer's because his framework was correct and powerful but could not cover every prime.

These failures modes required an ever greater depth of mathematical vocabulary even to be *stated*: one cannot articulate Euler's error without realizing that one needs to verify an assumed property of a more general number system; one cannot articulate Germain's without the concept of an infinite density condition on primes; and one cannot articulate Kummer's without the class number concept that his own theory created. The approach taken in this essay follows the interpretive line of Edwards (1977, preface), who read the theorem's history as a sequence of conceptual inadequacies whose repair constitutes the development of algebraic number theory. However, while Edwards used FLT to trace the genealogy of mathematics, the present essay makes a stronger historical claim that FLT was not merely a convenient narrative thread. Instead, it played an active role as the *occasion* on which each successive inadequacy became visible to the mathematical community.

Failure of method: Fermat and the limits of infinite descent

Fermat's only surviving proof relevant to FLT appears as a marginal note on Diophantus's *Arithmetica*, in which he proves by infinite descent that no right triangle with integer sides can have square area (Bachet 1670, Observation XLV; Edwards 1977, §1.5). This is equivalent to showing that $x^4 + y^4 = z^2$ has no positive integer solution, from which the $n = 4$ case follows since any fourth power is also a square. The proof begins by assuming a minimal solution (x, y, z), applies the parametrisation of Pythagorean triples, and invokes the principle that if a product of two coprime integers is a perfect square, each factor is individually a square. The decompositions yield a new triple with a strictly smaller value of z, contradicting minimality.

Two features are worth highlighting here. First, the proof operates entirely within $\mathbb{Z}$: its only tools are the parametrisation of Pythagorean triples and the unique factorisation of integers. Second, the method cannot scale. For an odd prime p, the factorisation $x^p + y^p = (x + y)(x^{p-1} - x^{p-2}y + \cdots + y^{p-1})$ produces a second factor of degree $p - 1$, and extracting a descent from it demands algebraic identities that grow intractable with p.

Fermat understood the latter limitation. In a 1659 letter to Pierre de Carcavi, he described applying descent to "affirmative questions" only with great difficulty (Fermat to Carcavi, August 1659, Œuvres, II, letter CI; translation in Fauvel and Gray 1987, §11.C7). That letter lists the cubic case of FLT among results proved by descent, alongside other claims like the two-squares theorem for primes of the form $4k + 1$. But it is the cubic case only; the general claim for all $n > 2$ appeared nowhere in the Carcavi letter and survives only in the marginal note, where Fermat asserts a "truly marvellous demonstration" without naming any method (Bachet 1670, p. 61). The gap is telling. Fermat could catalogue the cube case as a routine application of descent, but did not ascribe any technique to his more general statement, hinting that his relationship with FLT was more so that of a conjecturer who was extrapolating beyond his reach.

It was Euler who converted this implicit limitation into a named structural impossibility. Having independently proved $n = 3$ and published the proof in the *Algebra* (1770, Part II, Ch. XV), he wrote to Christian Goldbach: "the proofs for $n = 3$ and $n = 4$ are so different from one another that I do not see any possibility of deriving a general proof from them" (Euler to Goldbach, 4 August 1753, in Fuss 1843, I, p. 618; translation in Fauvel and Gray 1987, §14.C2(a)). FLT had diagnosed its first mathematical inadequacy: to the tools available to Fermat, descent over $\mathbb{Z}$ is irreducibly case-by-case, and arithmetic as practised in the integers has no mechanism for unifying these cases.

Failure of assumption: Euler and the unconscious extension of $\mathbb{Z}$

Euler's $n = 3$ proof advanced the problem by leaving $\mathbb{Z}$. The key step factors $x^3 + y^3$ by introducing a complex root of unity $\omega = e^{2\pi i/3}$, obtaining $x^3+y^3 = (x+y)(x+\omega y)(x+\omega^2 y)$. The factorisation takes place in what is now called the ring of Eisenstein integers $\mathbb{Z}[\omega]$, numbers of the form $a + b\omega$ with $a, b \in \mathbb{Z}$. Euler then applied the coprimality principle from the $n = 4$ case: if a product of two coprime elements is a cube, each factor is itself a cube. This yields a smaller cube; continued iteration then contradicts minimality. Euler's notation gestures at numbers involving $\sqrt{-3}$, but his operations require the strictly larger ring $\mathbb{Z}[\omega]$.

He neither notices nor needs the distinction, because the question "which number system am I working in, and does unique factorisation hold there?" had not yet been posed.

The historically significant feature here is that Euler imported unique factorisation into $\mathbb{Z}[\omega]$ without recognising it as an assumption that needed to be verified. Unique factorisation does hold in $\mathbb{Z}[\omega]$, since the ring is Euclidean under the norm $N(a+b\omega) = a^2 - ab + b^2$, so the proof can be made rigorous. But Euler had no way of knowing *why* it holds. As Edwards observed, Euler never considered the question of unique factorisation in this domain; he "simply used it" (Edwards 1977, §2.2). The invisibility of the assumption was itself the diagnosis: the concept of a number system whose structural properties require explicit verification had not yet been isolated. Fermat knew his method was limited; Euler did not know he was relying on an unverified presupposition. The proof circulated unchallenged for decades through the widely read *Algebra*, and the hidden assumption went unnoticed until Kummer's generation. This delay marked the evolution of a mathematical culture where number domains were taken as given into one where their structural properties became objects of investigation.

Failure of reach: Germain and the ceiling of $\mathbb{Z}$

Germain's approach was qualitatively different from those of her predecessors. She designed a systematic programme of sufficient conditions, with a structured research strategy, identifiable subgoals, and an explicit criterion for completion. Germain worked in substantial isolation due to her position as a woman (Laubenbacher and Pengelley 2010, pp. 641–645). It is tempting to read her attraction to a problem of such public fame as partly strategic. In her letter to Gauss of 12 May 1819, she outlined what Laubenbacher and Pengelley (2010, p. 651) described as her "grand plan": for each odd prime p, she would try to show that infinitely many auxiliary primes θ of the form $2Np+1$ satisfy two conditions: (i) no two p-th power residues, modulo θ, are consecutive, and (ii) p is not itself a p-th power residue modulo θ, thereby forcing that in any solution to $z^p = x^p + y^p$, at least one of x, y, z is divisible by p^2 (Germain to Gauss, 12 May 1819; Del Centina and Fiocca 2012, pp. 689–693).

This work remained unpublished during Germain's lifetime, in part because she could not close the gap to make it a full proof. Her theorem entered the literature only through Adrien-Marie Legendre, who included a version attributed to her in his 1823 supplement to the *Théorie des nombres*, detaching the result from the broader programme Germain had architected (Edwards 1977, §3.2; Ribenboim 1979, lecture IV, §2). The letter to Gauss, therefore, remains our primary window into Germain's strategic thinking. It stated the obstruction precisely: "I have never been able to reach infinity, although I have pushed the limits far back" (Germain to Gauss, 12 May 1819). She added: "we need the infinite and not the very large" (ibid.).

The failure is one of scope rather than of false presupposition. Germain makes no incorrect assumption; her reasoning within $\mathbb{Z}$ is entirely sound. An infinite collection of primes of the requisite form does exist: Peter Gustav Lejeune Dirichlet's theorem on primes in arithmetic progressions (1837) guarantees that there are infinitely many primes of the form $2Np+1$ for any fixed p. However, Dirichlet's theorem was not enough. Germain required that infinitely many such primes also *simultaneously* satisfy her two residue conditions, a strictly harder requirement that Dirichlet's theorem does not address and that remains unresolved for general p up to this day. Germain could not have resolved her gap with more mature mathematical machinery; instead, that gap exposed the structural limitations of arguments that worked within the confines of $\mathbb{Z}$. Euler had left $\mathbb{Z}$ without realising it, and this departure was the source of his unexamined presupposition. Germain remained within $\mathbb{Z}$ consciously and systematically, and her failure demonstrates that remaining there is insufficient in principle.

Germain's letter to Gauss was also an occasion in the social sense. She used FLT as the vehicle through which to present her broader theory of residues to the one mathematician whose approval could legitimate her work, and the theorem functioned as an occasion not only mathematically, but institutionally—providing the pretext for a correspondence that would otherwise have been exceedingly difficult for a woman to sustain.

Failure of generality: Kummer and the limit that names itself

Kummer began precisely where Germain refused to go: outside $\mathbb{Z}$. In March 1847, Gabriel Lamé announced to the Paris Academy a purportedly general proof of FLT by factoring x^p+y^p into linear factors $(x+\omega^k y)$ over the cyclotomic integers $\mathbb{Z}[\omega]$, where now $\omega = e^{2\pi i/p}$, and running descent on coprime factors. The argument requires unique factorisation in $\mathbb{Z}[\omega]$. However, Kummer's letter to Joseph Liouville of 28 April 1847, published in the *Journal de mathématiques pures et appliquées* that same year, demonstrated that this precise requirement could not be satisfied: the "elementary proposition" that a composite complex number can be decomposed into primes in only one way "does not generally hold true" in $\mathbb{Z}[\omega]$ (Kummer to Liouville, 28 April 1847; translation on BO1.1 HT26 course webpage). For $p = 23$, elements of $\mathbb{Z}[\omega]$ exist that are irreducible but not prime, producing non-unique factorisations (Edwards 1977, §4.1).

Irreducibility and primality, equivalent in $\mathbb{Z}$ by the Fundamental Theorem of Arithmetic, separate in $\mathbb{Z}[\omega]$ for $p \geq 23$. Lamé's proof collapses at precisely this point, and the collapse reveals that unique factorisation, accepted as a universal property of numbers since Euclid, is in fact a local property of $\mathbb{Z}$.

Both Euler and Lamé failed by importing unique factorisation into an extended domain without verification. Seventy years after Euler's proof, FLT functioned, once again, as the *occasion* that brought a long-hidden assumption into the open, revealing the failure of unique factorisation in cyclotomic integers. Liouville's editorial note, which treated the matter as immediately worthy of the journal's attention, demonstrated how quickly the mathematical community recognised the seriousness of the gap (Liouville's note in *Journal de mathématiques pures et appliquées* 12, 1847, p. 136)—driven, in no small part, by the notability of progress on this theorem.

Kummer's response was to rebuild. His letter announced that unique factorisation "can be salvaged by introducing a new kind of complex number that I have called an ideal complex number" (Kummer to Liouville, 28 April 1847). The construction works by studying the elements ideal numbers divide rather than writing them down explicitly, an approach that Richard Dedekind would later reformulate by identifying ideal numbers with the sets of multiples they determine (Edwards 1977, §4.1; Gray 2018, ch. 16). Using ideal numbers, Kummer proved FLT by 1850 for all *regular* primes: primes p for which p does not divide the class number of $\mathbb{Z}[\omega]$. This establishes FLT for all primes up to 100 except for the three cases of 37, 59, and 67. Yet, for *irregular* primes, the descent argument cannot be forced to close, and no elementary extension of Kummer's method handles these cases. Unlike Fermat's failure, where his method of infinite descent did not work aside from a single case, Kummer's failure—and the regular/irregular distinction that it revealed—was only evident after he created a new and comprehensive framework to tackle FLT.

Here, this essay's thesis meets its most serious complication. Edwards argued that the idea Kummer was mainly led to ideal numbers by FLT "is surely mistaken": Kummer's notation, methods, and immediate mathematical context were all derived from Carl Gustav Jacob Jacobi's work on higher reciprocity laws (Edwards 1977, p. 79). The thesis that FLT is a diagnostic instrument must therefore be stated carefully. It is true that no single mathematical hypothesis drives the evolution of an entire field; that progress is necessarily caused by an intersecting web of occasions of varying characters; that mathematical progress is combinatorial. FLT did not *cause* the invention of ideal numbers; reciprocity was the most proximal motive. However, FLT is a key occasion in that intersecting web—and a uniquely important one owing to its enigmatic history. Lamé's failed proof, motivated entirely by FLT, was the *occasion* that publicly revealed the failure of unique factorisation in cyclotomic integers, and Kummer's letter to Liouville is the document in which this revelation was made precise. FLT's role was that of an occasion for visibility rather than a cause of invention. That the diagnosis required public occasions—Lamé's Academy announcement, Liouville's editorial intervention, and Kummer's published reply—where Euler's identical error had circulated unchallenged for seventy years through the *Algebra*, illustrates how the visibility of a structural inadequacy depends on the institutional conditions of its reception as much as the novelty of the mathematics itself.

Conclusion

The four failure modes form a coherent progression where each operates at a higher level of mathematical abstraction than the last. The diagnostic power of FLT is derived from its persistence across these convenings. Diophantus's *Arithmetica* (Book II, Problem 8) asked for a decomposition of a given square into two rational squares (Bachet 1670, p. 61; Christianidis and Oaks 2023, pp. 300–314); Fermat's note generalized this constructive problem into a universal impossibility over the integers. This transformation is what made FLT dialectically potent. Yes, Gauss predicted that FLT would appear as a mere corollary, and Wiles's proof, nearly two hundred years later—which establishes the modularity of semistable elliptic curves and obtains FLT as a consequence (Wiles 1995)—vindicated that prediction. But the developments that made FLT a corollary were themselves shaped by the pressure the theorem exerted: cyclotomic field theory and the theory of ideals were developed partly in response to failures encountered in Fermat's setting, and even Wiles's proof of modularity for semistable curves was directly motivated by the Frey–Ribet connection to FLT (Edwards 1977, chs. 4–6; Gray 2018, ch. 16). What Gauss dismissed as an isolated result turned out to be a statement whose very simplicity ensured that it would be encountered again and again, and whose depth ensured that each encounter would expose the limits of whatever framework was brought to bear.

Fermat's Last Theorem did not passively await a theory large enough to contain it. Instead, it became the occasion, repeatedly, for discoveries that the existing theories were inadequate; and the winding ladder of those discoveries, not the theorem itself, wove the web with contemporary progress in mathematics to create what we now know as algebraic number theory.

Bibliography

Primary sources

Bachet de Méziriac, Claude-Gaspard (ed.), *Diophanti Alexandrini Arithmeticorum libri sex*, with Pierre de Fermat's Observationes, Toulouse: Bernard Bosc, 1670.

Christianidis, Jean, and Jeffrey Oaks (eds.), *The Arithmetica of Diophantus: a complete translation and commentary*, Routledge, 2023.

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

Fermat, Pierre de, *Œuvres de Fermat*, ed. Paul Tannery and Charles Henry, 4 vols., Paris: Gauthier-Villars, 1891–1912.

Fuss, P. H. (ed.), *Correspondance mathématique et physique de quelques célèbres géomètres du XVIIIème siècle*, 2 vols., St Petersburg, 1843.

Gauss, Carl Friedrich, and Wilhelm Olbers, *Briefwechsel zwischen Olbers und Gauss*, ed. C. Schilling, Berlin: Julius Springer, 1900 (Erste Abtheilung).

Germain, Sophie, letter to Carl Friedrich Gauss, 12 May 1819; French text 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 (pp. 689–693); English translation by Christopher Hollings, available on the BO1.1 HT26 course webpage.

Kummer, Ernst Eduard, letter to Joseph Liouville, 28 April 1847, published in *Journal de mathématiques pures et appliquées* 12 (1847), 136; reprinted in *Collected papers*, ed. André Weil, 2 vols., Springer, 1975, vol. 1, p. 298; English translation by Christopher Hollings, available on the BO1.1 HT26 course webpage.

Wiles, Andrew, 'Modular elliptic curves and Fermat's Last Theorem', *Annals of Mathematics* 141 (1995), 443–551.

Secondary sources

Edwards, Harold M., *Fermat's last theorem: a genetic introduction to algebraic number theory*, Springer, 1977.

Fauvel, John, and Jeremy Gray, *The history of mathematics: a reader*, Macmillan, 1987.

Goldstein, Catherine, and Norbert Schappacher, 'A book in search of a discipline (1801–1860)', in *The shaping of arithmetic after C. F. Gauss's Disquisitiones arithmeticae* (Catherine Goldstein, Norbert Schappacher, and Joachim Schwermer, eds.), Springer, 2007, 3–65.

Gray, Jeremy, *A history of abstract algebra*, Springer, 2018.

Laubenbacher, Reinhard, 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.

Laubenbacher, Reinhard, and David Pengelley, *Mathematical expeditions: chronicles by the explorers*, Springer, 1999.

Mahoney, Michael Sean, *The mathematical career of Pierre de Fermat, 1601–1665*, 2nd ed., Princeton University Press, 1994.

Ribenboim, Paulo, *13 lectures on Fermat's last theorem*, Springer, 1979.