Fermat’s Grandest Claim

Final Paper

MATH 491

12/13/2021

Ryan Morganti

**Abstract**

“I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain.”[[1]](#footnote-2) This seemingly innocent statement alluding to a proof by Pierre de Fermat led mathematicians on an over three-hundred-year hunt trying to replicate it. Since this claim was made public in the publishment of Fermat’s annotated copy of *Arithmetica* by the ancient Greek, Diophantus of Alexandria, mathematicians tried their intellect against the corresponding proposition: for any integer n greater than 2 there is no integer solution. Their attempts went to lead revolutions in number theory and new ways of solving numeric problems. The quest went so far as shaping people’s lives through their dedication and determination to take on the “holy grail” of mathematics. This paper will discuss the mathematical concepts surrounding this theorem, the cases of n=3 and n=4 as well as the general proof.

It is a well-known fact that for there are infinitely many solutions for where are integers. For n=1 we have any number of possibilities to choose from, e.g., . For n=2, we also have any number of possibilities. This was proven by Pythagoras with the Pythagorean Theorem. Answers that satisfy , like , are called Pythagorean Triples. However, Fermat was the first to extrapolate, and claim a solution to, any number . There is contention if Fermat produced a correct, complete proof, if he had a flaw in his proof, or if he simply never had a proof. And even if Fermat had a correct proof, his methods would have been centuries behind modern ones, meaning his method would have been one so ingenious that the math world never dreamed of it in over three hundred years.[[2]](#footnote-3) These methods would have all been results of basic algebra principles and geometric properties involving simple two- and three-dimensional shapes, as well as arguments along the lines of contradiction, infinite descent, or induction. Modern methods and results in algebraic geometry, structures, and fields, (all used in the modern proof), would have been inaccessible to Fermat. Whatever the case, the difficulty behind this problem is that the domain to check is so large. There are an infinite amount of numbers to check, and methods like induction fail to work since there is no obvious way to sequence a chain such that if it works for some number then it must also hold for . Even with centuries of mathematicians working, and more modernly, computers, it took ingenuity and a series of breakthroughs to finally end the question and prove Fermat correct.

Even if the general solution had to wait a few hundred years, special cases would be proven, starting with the case n=4, given by Fermat himself.

**Case of n=4**

Even though Fermat failed to provide a general proof, his other works can be applied to yield the result of the special case of n=4. To prove this case, Fermat described a new mathematical proof, infinite decent. This technique assumes the well-ordering principle, that there is a smallest answer, and finds a chain of events that finds a smaller solution. This chain of events goes of infinitely, meaning there is no smallest solution, which is a contradiction. Fermat incorporated this idea into the proof for the special case of n=4, which is as follows.

Proof:

Instead of showing has no integer solution, it is easier and equivalent to show that has no integer solution. This follows from the fact that . If is not a solution, then it is impossible for to be a solution either. Assume by contradiction that holds, that and that is the smallest possible solution to exist. Note that the pair is a Pythagorean triple.

Claim: and in a Pythagorean triple have opposite parities

Let be a Pythagorean triple. Since they are a Pythagorean triple, with ,. Consider a number . If is even, we have since for an integer. Otherwise, if is odd, we have since for an integer. Assume that both and are odd, then which is impossible since ever. If both and  are even, then is also even, which is another contradiction since . Therefore and must have opposite parities.

Since is a Pythagorean triple, and have opposite parities. Without loss of generality, assume that is odd and is even. This implies that is therefore odd as well. For two coprime numbers write:

Then rewrite which is another Pythagorean triple. Thus, there exists another two coprime numbers such that the following is true:

Claim: If the product of two positive integers, that are relatively prime, is a perfect square, then each individually is a perfect square.

Let for positive integers with and relatively prime. Since is a square, every prime factor will appear an even number of times. Further, since , and share no factors. This means that every prime factor in and will appear an even number of times. This means that they are both squares as well.

Using the above claim, both and are perfect squares since . Furthermore, , and since is a perfect square, by lemma 2, and are squares. Let the following be the results:

Then can be rewritten as . Consider again . Then so this is a smaller solution. This is a contradiction since it was assumed that was the smallest solution. Therefore, has no solution.

**Case of n=3**

It took over a hundred years before the next case was proven by Leonard Euler. Euler adopted Fermat’s infinite descent method to show the case of n=3. Before the proof, consider two claims.

Claim: If , and then there exists such that .

Assume that , and . Also assume by contradiction that , meaning is not an n-power of any number. Thus as . By the fundamental theorem of arithmetic, is divisible by some prime . Write for an integer.

Also, divides since . By definition of divides, for m an integer. Then,

Which can be rewritten as . So either divides or . cannot divide since divides and , thus divides . Since can only divide , it follows that must also divide . By definition of divides, for an integer. Then,

Which can be rewritten as . since is a divisor of (as divides which divides ) and . cannot be an n-power either, since if it were, would make an n-power. is less than since and . Therefore, we have contradiction by using infinite descent.

Claim: In the equation , x, y, and z are all coprime with each other, or the equation can be reduced such that x, y, and z are all coprime to each other.

If x, y, and z are all coprime to each other, then there is nothing to show, so assume that at least two of them are not coprime. We will start by showing that if a factor divides any two values of , then the n-power of the factor divides the n-power of the remaining value. Break into two cases.

Case I:

Assume that and are not coprime, then there exists an integer such that divides and . Thus, there exists and where and . By substitution:

And by definition divides .

Case II:

Assume and are not coprime or and are not coprime. Without loss of generality assume that and are coprime. Then there exists an integer such that divides and . This means that and . By substitution:

And by definition divides .

Now we will show that if divides , it means that divides . Let , then there exist integers where and . Since is taken to be the then and by definition. Since divides , for k an integer. This becomes

Then . To show this, assume that with . This means that divides and by associativity, divides . Above we said that so this is a contradiction. Using the above claim (If , and then there exists such that ), is an n-power and there exists such that . Thus, we have which implies Multiply by , so , meaning divides .

This shows that divides all and so the equation can be simplified to where they are all coprime.

The following Euler’s proof for n=3, which contains an error. When he introduced the imaginary number , he skipped over the fact that in that field there is no unique factorization.[[3]](#footnote-5) This derails the argument that it must break down into being made of cubes. Even though Euler missed this fact, his other works can be used to remedy this and salvage the proof. The fix uses the lemma by Edward: Let and be relatively prime numbers such that is a cube. Then there exist integers and such that .[[4]](#footnote-6) Applying a slightly modified version of this, along with the proof showing the number is necessarily smaller, the proof is fixed and accurate.

Proof:

Assume by contradiction that there is a solution to for . This statement has equivalent value to , so we need to show that either the sum or difference of cubes results in a cube. Using the above claim, assume that the equation has been simplified so that are all coprime to each other. Since they are coprime, then either and are both odd or one even and one odd. In the case that they are both odd, will be even, and in the other case will be odd. It is sufficient to assume the case where both and are both odd, since otherwise the equation can be arranged as , which is necessarily equivalent.

Let and . This can be rewritten as and . It follows that both and must have different parities since and are odd, and the way to get that is by adding an even and odd number together. Write:

In the same way, the difference of cubes is necessarily the same equation:

Since is even and a cube, it must be divisible by 8. Meaning that is a whole number. To satisfy this, must be even and odd. Thus is even. Since and are relatively prime, then and must only have shared factors of 1 or 3. Break into cases.

Case I:

Assume p is not divisible by 3, then the only common factor is 1, therefore and are relatively prime. By the claim, if , and then there exists such that , both and are cubes. Next, we will look at the extension into . Then it is possible to factor as . If either or are cubes, we have:

and

After multiplying

By expansion of , we have

With equating the imaginary and real components, we have

and

Since is odd, it follows that must also be odd and even. Since must be a cube and thus a cube as well, then must be a cube as well. Since is even and not divisible by 3, then , , and must all be relatively primes and by lemma 1, cubes. Write:

Then since is also a cube, then it is a sum of cubes. Both and are strictly smaller than the original and , so a smaller solution can be found. Using infinite descent this can continue, which is a contradiction since there must be a smallest possible answer.

Case II:

Assume that p is divisible by 3, and write , then:

Now both and are relatively prime since the latter cannot be divided by 2 or 3 and must be even by being even. From the Case I:

Since is odd, must also be odd and even. Also, by lemma 1, must be a cube. Multiply that by the cube and get:

This must also result in a cube by lemma 1, so consider:

This is like the first case. Apply the method of infinite descent and a smaller solution will keep being found. This results in a contradiction.

Since both cases lead to a contradiction, the original assumption must be false and there are no possible solutions to either or .

**Cases of n being prime:**

Since both proofs are quite different in their workings, mathematicians were stuck trying to apply these techniques to the general case. The next breakthrough occurred seventy-five years later. Sophie Germain suggested methods to take down many cases at once. She broke Fermat’s Last theorem into two separate cases with an odd prime:

Case I: are pairwise coprime with

Case II: are pairwise coprime with

It became only necessary to look at prime cases since any higher order composite can be broken into primes e.g., . If it could be proven for the prime powers, then it would necessarily result in the composite numbers being proven as well. Sophie Germain took this idea and looked at auxiliary primes, which are primes related to another prime , of form . For example, 31 is an auxiliary prime to 5 since . Likewise, the special case of such that is also a prime, is called a Germain Prime. Sophie Germain described the following proof, but Adrien Legendre was the one to actually provide the proof.

Proof:

Suppose that is an odd prime and that is also prime. We want to show that the Case I of Fermat’s Last Theorem holds for . Assume by contradiction that are pairwise coprime and a solution to the Case I of Fermat’s Last Theorem. Using the Binomial Theorem, . Since by assumption, it follows that either.

Claim: Let be coprime integers and an odd prime, then or

Let , then using a binomial expansion. Since , Fermat’s Little Theorem states that . Further, every term is divisible by by definition. There are two cases, either divides and thus divides or does not divide and thus does not divide either. In the former, that would mean . In the latter, that would mean .

Since , . Since , it is equivalent to write . This means that is a product of coprime integers. Using the result (if , and then there exists such that ), we have:

and

Using the same process for and , the results are:

Claim:Let be a Germain Prime with and . Then at least one of is divisible by .

Suppose by contradiction that none of are divisible by . Using Fermat’s Little Theorem . Also, . Equating these two, . Solving this yields . Using our assumption that and the found value of , then which is impossible under our assumptions, a contradiction.

Without loss of generality, assume that exactly one of say is divisible by , then:

Thus which is equivalent to . Again, using the above claim, must divide one of . Also, since , then . It follows that which is equivalent to . This means the following is true:

Therefore, it follows that

This contradicts and so the assumption is false.

Corollary: Suppose that is an odd prime and an auxiliary prime. mod q implies at least one of is divisible by if and only if the list of pth powers modulo contain no consecutive non-zero integers.

We will show a proof by contrapositive. The list of pth powers modulo contains consecutive non-zero integers, if and only if and are not divisible by .

Assume that and are not divisible by . Thus, there exists an integer where . Multiply by

Thus, there are two consecutive non-zero integers of pth powers.

Assume that there are non-zero consecutive pth powers, and where . Since both of these are non-zero modulo , then and must also be non-zero modulo . Also, which is equivalent to . Therefore, there exists integer of the form where are not divisible by .

Since the contrapositive of the claim holds, the original statement holds.

Using the corollary applied in the proof above, Case I could be applied to a whole range of integers for Fermat’s Last Theorem. All that would need to be found is a suitable auxiliary prime. For example, when , there is an auxiliary prime . Then . Since there are no consecutive pth powers, then the claim above says mod q implies at least one of is divisible by . This can then be used within the original proof to show that Case I of Fermat’s Last Theorem is true for . This narrowed down Fermat’s Last Theorem to finding suitable auxiliary primes.

Legendre would take Germain’s work and apply it to a more general case that both cases 1 and 2 hold whenever at least one of is also a prime for any prime .[[5]](#footnote-9) Between Legendre and Germain, Fermat’s Last Theorem was solved for all . As the numbers grew, finding auxiliary primes and calculating the consecutive terms became impossibly hard to find by hand.

**Cauchy, Lamè, Kummer, and Ideal Theory**

Both Augustin Louis Cauchy and Gabriel Lamè announced in 1847 at the Academy of Paris that they were on the verge of cracking Fermat’s Last Theorem and their proofs were almost complete. Lamè based his work on a concept called the roots of unity. These are complex numbers, say such that . For example, when , is a root of unity since . By utilizing these numbers in the equation , then each is pairwise coprime with the rest. This can lead to an infinite decent argument by continuing this process. Cauchy’s work followed along similar lines and also contained a portion that relies on the unique factorization into primes particular in the field . This factorization uses cyclotomic integers, which are roots of unity for complex numbers with form for a prime number and imaginary root In rings that have complex components, unique factorization into primes does not exist. Kummer would prove that for this ring does not factor uniquely, due to an argument that involves class numbers of cyclotomic integers.

An easier example of non-uniqueness of factorization is in the ring . Consider the element . To be unique, the factorizations must have irreducible elements with unique norms. An element is considered irreducible if implies that either or is a unit. Let the norm of an element be defined as . Then in the example above, both factorizations are into irreducible elements and have norms . The norms are unique. They cannot be factored further since there is no possible element where .

Lamè and Cauchy both tried to remedy this issue of uniqueness but were ultimately unsuccessful. Even though Cauchy and Lamè gave up on their proposed solutions, Kummer was able to salvage their proofs for some specific cases. Kummer did this by looking at numbers that he called “ideal” with properties that if the ideal number divides , then it also divides . Also, if it divides and , then it divides . Kummer proved Lamè’s result in cases where the class number of the cyclotomic number field is 1. The only numbers that were solved this way were 3, 5, 7, 11, 13, 17, and 19. Furthermore, a weaker case can be applied for regular primes. These are primes such that does not divide the class number. This reduced Fermat’s Last Theorem to needing to be proved for only irregular primes, the lowest one being 37.

The concept of ideals was further investigated by Richard Dedekind who flushed out the idea fully. Let be a ring, and and ideal of . Then is a subset of with the properties: if then , and if and then .[[6]](#footnote-11) This would lay the foundation for modern algebraic number theory and the study of ideal theory. Using the idea of ideal theory, the following is a result of fixing unique factorization in the given ring above.

Let be the ideals generated by those elements. Then, is an ideal generated by those four elements with every element in having the form . Since each element in is divisible by Likewise, because . Therefore . Likewise, using the same logic and equivalences, the following are true as well . Therefore, we arrive at the conclusion that . And no matter which factorization is used, the result is the same. This means that 6 has a unique factorization, and the issue with unique factorization has been restored when applied to ideals.[[7]](#footnote-12)

**Advancement in Elliptic Curves and Modular Forms**

Two important results that would lead to the solving of Fermat’s Last Theorem are in seemingly unrelated studies of mathematics. The first is the study of elliptic curves. An elliptic curve is an equation of the following form, . An example elliptic curve is which looks similar to a sideways Ω when graphed. These curves can be encoded into an L-series which uses a sum of primes found within the curve.

Now consider the seemingly unrelated concept of modular forms. Modular forms are functions where . is also known as the upper-half space. This function must also have the following properties[[8]](#footnote-13):

1. is smooth, meaning it is continuous and infinitely differentiable
2. must be holomorphic, meaning it is differentiable for all elements in the set
3. Let , then for all and , with the weight of the modular form
4. The values of are bounded as

Modular forms also have an M-series which are described by .[[9]](#footnote-14) By looking at the ordering of both L-series and M-series of these two distinct groups, Yutaka Taniyama, and his friend Goro Shimura deduced that some matched up for a good portion of the values. They conjectured that this not only held true for certain cases, but that all elliptic curves had a corresponding modular form by equating these two series. They released their results in 1955 at a symposium in Japan, but it would take a decade before their work was generally accepted. This conjecture inspired a great movement in mathematics in the 1960s. Led by Robert Langlands, mathematicians sought to link all different mathematical fields together in a grand unification.[[10]](#footnote-15) Gerhard Frey linked the Taniyama-Shimura conjecture directly to Fermat’s Last Theorem.

**Fermat’s Last Theorem and the Taniyama-Shimura Conjecture**

In 1985, Gerhart Frey announced the result that tied the Taniyama-Shimura conjecture to Fermat’s Last Theorem. Frey took Fermat’s equation and through substitution and rearranging produced , an elliptic curve.[[11]](#footnote-16) Intuitively Frey figured out that this elliptic curve would be impossible to construct as a modular form due to its “strangeness”. However, he failed to prove why it was sufficiently “strange”. What followed was the work of Jean-Pierre Serre and Ken Ribet who proved that it was impossible to generate a modular form given the properties of the formed elliptic curve. Their work used Galois Theory, which is a way to study and relate field extensions into permutation groups for polynomial equations solvable into radicals.[[12]](#footnote-17) With this new result, Fermat’s Last Theorem became linked to the results of the Taniyama-Shimura conjecture; if one was proven true the other would automatically be proven false. The math community has a strong sense that the Taniyama-Shimura conjecture would be proven true in the relative future, meaning that whoever could prove that conjecture would prove Fermat’s original claim once and for all.[[13]](#footnote-18)

The person who finally tackled this conjecture was Andrew Wiles. He spent seven years working in secrecy, much like Fermat, writing his proof. In a three-part lecture simply titled, “Modular Forms, Elliptic Curves and Galois Representation”, given at a conference held at the Isaac Newton Institute in June of 1993, Wiles unveiled his proof to the world.[[14]](#footnote-19) Wiles combined the latest results in number theory into an induction proof. By using the methods described by Kolyvagin-Flach, Wiles developed a lengthy argument that systematically compared modular forms and elliptic curves. However, in his initial draft, he made a mistake and assumed that the method he employed was able to work for all cases, which it could not. By examining Iwasawa theory and uniting it the Kolyvagin-Flach method, Wiles was able to salvage his proof, and proved that the Taniyama-Shimura conjecture was true. This meant that Fermat’s Theorem was also proven, and finally more than three-hundred years later the greatest question in mathematics was solved.

For centuries Fermat tormented the math community. It took centuries of work and the use of 20th century techniques to finally bring the question to the ground, once and for all proving that has no integer solutions for . Pierre de Fermat was finally proven right, vindicating his claim. Although Fermat himself may have never produced a proof, the treasure hunt that he started revolutionized number theory, changed people’s lives, and linked together totally different fields.

References

“A special case of Fermat's Last Theorem, where n=3.” *YouTube*, uploaded by

Maths Explained, 21 Jun. 2021, <https://www.youtube.com/watch?v=ij5imAf0B0E>

Byerley, Cameron. *Application of Number Theory to Fermat's Last Theorem*.

<https://www.whitman.edu/Documents/Academics/Mathematics/byerleco.pdf>.

Corn, Patrick, and Jimin Khim. “Elliptic Curves.” *Brilliant Math & Science Wiki*,

<https://brilliant.org/wiki/elliptic-curves/>.

Darmon, Henri, et al. *Fermat's Last Theorem*. <https://people.math.wisc.edu/~boston/ddt.pdf>.

Edwards, Harold M. *Fermats Last Theorem: a Genetic Introduction to Algebraic Number Theory*.

Springer, 1996.

*Elliptic Curves*. <http://www-math.ucdenver.edu/~wcherowi/courses/m5410/elliptic.pdf>.

*Elliptic Curves*. <https://www.cs.purdue.edu/homes/ssw/cs655/ec.pdf>.

“Elliptic Curves and Modular Forms | The Proof of Fermat’s Last Theorem.” *YouTube*, uploaded by

Aleph 0, 26 Jul. 2020, <https://www.youtube.com/watch?v=grzFM5XciAY>

“Fermat's Last Theorem.” *Maths History Club*,

<https://www.mathshistoryclub.com/2021/07/ferrmats-last-theorem.html>.

*Fermat's Last Theorem for Regular Primes*.

[https://math.berkeley.edu/~sander/speaking/22September2015 WIM Talk.pdf](https://math.berkeley.edu/~sander/speaking/22September2015%20WIM%20Talk.pdf).

*Fermat's Method of Descent*. <https://www.math.uci.edu/~ndonalds/math180b/5descent.pdf>.

Freeman, Larry. *Fermat's Last Theorem: n = 3: Step 3*, 26 May 2005,

<https://fermatslasttheorem.blogspot.com/2005/05/fermats-last-theorem-n-3-step-3.html>.

Gong, Ting. *Modular Forms*. 18 May 2020,

<https://sites.nd.edu/ting-gong/files/2020/05/modular-form.pdf>.

Hewlett, John, and Scott L. Hecht. *Elements of Algebra*. Createspace, Inc. & Kindle Direct Publishing,

2015.

“Holomorphic Function.” *Brilliant Math & Science Wiki*, <https://brilliant.org/wiki/holomorphic-function/>.

*Introduction - Fermat's Last Theorem: n=4*,

<https://crypto.stanford.edu/pbc/notes/numberfield/fermatn4.html>.

“Kenneth A. Ribet, ‘A 2020 View of Fermat’s Last Theorem’.” *YouTube*, uploaded by Joint Mathematics

Meetings, 3 Feb. 2020. <https://www.youtube.com/watch?v=grzFM5XciAY>

Koblitz, Neal. *Introduction to Elliptic Curves and Modular Forms*. Springer, 1993.

*L-Series of an Elliptic Curve*. <https://planetmath.org/LSeriesOfAnEllipticCurve>.

Magner, Ricky. *Ribet's Level-Lowering Theorem for Modular Representation*.

<https://math.bu.edu/people/rmagner/extras/RibetLevelLowering.pdf>.

*Modular Forms*. [https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016 /02/CTNTmodularforms.pdf](https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016%09/02/CTNTmodularforms.pdf).

Mordell, Louis Joel. *Three Lectures on Fermat’s Last Theorem*. 1962.

Pellegrino, Daba. “Pierre De Fermat.” *History of Mathematics Research Paper, Spring 2000*, Rutgers,

<https://sites.math.rutgers.edu/~cherlin/History/Papers2000/pellegrino.html>.

*Resource E: Fermat's Last Theorem for n=4*.

<https://www.maths.tcd.ie/pub/Maths/Courseware/EllipticCurves/2016/Fermat-n4.pdf>.

Ribet, Kenneth A. *News Item for the "Notices of the American Mathematical Society"*.

<https://math.berkeley.edu/~ribet/Articles/notices.pdf>.

Schettler, Jordan. *An Introduction to Iwasawa Theory*. <https://web.math.ucsb.edu/~jcs/History.pdf>.

Silverman, Joseph H. *An Introduction to the Theory of Elliptic Curves*.

<https://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve.pdf>.

Singh, Simon. “The Whole Story.” *Simon Singh's Website*,

<https://simonsingh.net/books/fermats-last-theorem/the-whole-story/>.

Singh, Simon, and John Lynch. *Fermat’s Last Theorem: The Story of a Riddle That Confounded the*

*World’s Greatest Minds for 358 Years*. Harper Perennial, 2011.

*Sophie Germain and Fermat's Last Theorem*.

<https://www.math.uci.edu/~ndonalds/math180b/6germain.pdf>.

“Taniyama-Shimura Conjecture.” *From Wolfram MathWorld*,

<https://mathworld.wolfram.com/Taniyama-ShimuraConjecture.html>.

“The n=4 Case of Fermat's Last Theorem.” *Question Corner -- The n=4 Case of Fermat's Last Theorem*,

<https://www.math.toronto.edu/mathnet/questionCorner/fermat4.html>.

“What is the square root of two? | The Fundamental Theorem of Galois Theory.” *YouTube*, uploaded by

Aleph 0, 25 Nov. 2021, <https://www.youtube.com/watch?v=CwvuZ8aHyH4>

1. Simon Singh the Whole Story [↑](#footnote-ref-2)
2. Fermat’s Last Theorem – A Genetic Introduction to Algebraic Number Theory pg 2 [↑](#footnote-ref-3)
3. Applications of Number Theory to Fermat’s Last Theorem [↑](#footnote-ref-5)
4. Fermat’s Last Theorem: A Genetic Introduction to Algebraic Number Theory [↑](#footnote-ref-6)
5. Sophie Germain and Fermat’s Last Theorem [↑](#footnote-ref-9)
6. Algebraic Number Theory pg 73 [↑](#footnote-ref-11)
7. Fermat’s Last Theorem for Regular Primes [↑](#footnote-ref-12)
8. Modular Forms [↑](#footnote-ref-13)
9. Elliptic Curves and Modular Forms | The Proof of Fermat’s Last Theorem [↑](#footnote-ref-14)
10. Fermat’s Last Theorem page 134 [↑](#footnote-ref-15)
11. Fermat’s Last Theorem page 138 [↑](#footnote-ref-16)
12. What is the square root of two? | The Fundamental Theorem of Galois Theory [↑](#footnote-ref-17)
13. Ken Ribet - Notices [↑](#footnote-ref-18)
14. Fermat’s Last Theorem pages 168-169 [↑](#footnote-ref-19)