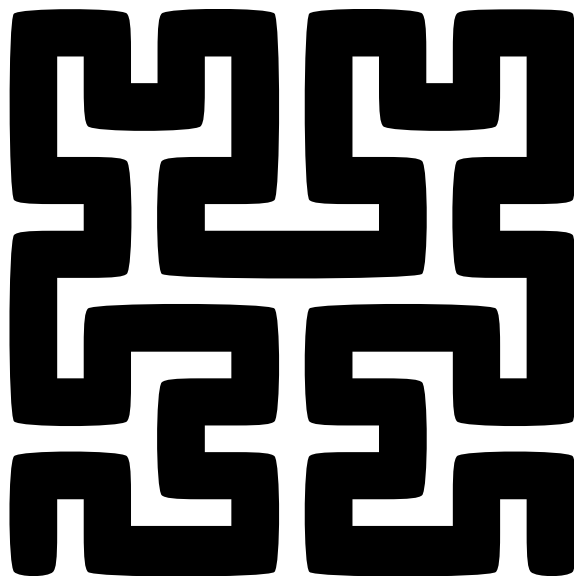




Polynesian Journal of Mathematics

Volume 4, Issue 5

Special volume AĴAX in honor of René Schoof

René Schoof's mathematical maps

Capi Corrales Rodrigáñez

Received 18 Jan 2026

Revised 11 Mar 2026

Accepted 12 Mar 2026

Published 28 Sep 2026

Communicated by Elisa Lorenzo García

DOI: 10.69763/polyjmath.4.5

René Schoof's mathematical maps

Capi Corrales Rodrigáñez

Departamento de álgebra, geometría y topología
Facultad de Matemáticas, Universidad Complutense de Madrid, Spain

Abstract

Planning our first visit to a new land is not that different from the task that mathematics students must face when starting their research training. For such a task, traditional road maps that can be unfolded in front of our eyes are needed. As we will explain in these pages through some concrete examples, René Schoof's expository papers offer a varied catalogue of road maps of some the most beautiful territories developed in number theory.

These pages are aimed at mathematics students in the early stages of their research training and their advisors, as well as to René Schoof (they were conceived as a gift for him) and his friends.

1 Introduction

It was 2005 and I was teaching an introductory course in number theory at *Universidad Complutense de Madrid*. Each student was supposed to choose a topic and prepare an oral presentation to be given in front of the group. While listening to one of them I felt from the beginning as if attending a lecture by René Schoof. Even though the student was speaking in Spanish, the narrative was undoubtedly Schoof's. I interrupted him several times with questions; each time, after a quick "I don't know," he would resume his presentation picking it up exactly where he had left it, as if declaiming a poem. I finally asked the student whether he had literally translated into Spanish a text written by René Schoof and then learned it by heart. Too shocked to deny it, a question escaped from his lips, "How did you know?" The last thing that he expected was me hearing Schoof's voice behind his words. That morning I found out two things. First, that in 2005 René Schoof's expository papers were in the reading lists of most students at the mathematics department in *Complutense*, a fact that remains true today. Second, that I could recognize Schoof's mathematical style. I would like to reflect briefly on both.

The use of the driving navigation features in our mobile phones has trained most of us off the use of road maps with which to plan our trips. These tools are very useful when we want to find out how to get to a precise address within a city or which roads to take when we want to go from one specific place to another. But they are of no

use when we want to plan a true voyage involving the exploration of new territories. Students aiming at doing research in mathematics must choose a field of study and a topic of research and it is difficult to make a sound choice without access to a broad, clear picture of the overall situation. Once they have made a choice, they will need to know which are the fundamental results that they must understand, learn how to use and relate to each other. In these steps, expository pieces play an essential role as navigation tools, road maps one could say.¹ René Schoof's stand as true jewels and I was not surprised to find them in the reading lists of most mathematics graduate students in *Complutense*. Written with great clarity, they often cover topics which are of actuality (e.g., [16, 18, 19]), essential for the understanding of algebraic number theory (e.g., [15, 17]) or both (e.g., [20]). Furthermore, the proofs of most of the results that he chooses to explain require a constant combination of classical and contemporary techniques; Schoof masterly exploits this fact, constructing the logical structures that characterize his arguments, as elegant as illustrative of the evolution of the mathematics involved. His ability to find beautiful new examples with which to introduce abstract concepts and results and motivate their study is truly remarkable (e.g., [15, 17]).

All these features make René Schoof's mathematical expositions valuable navigation tools to study with as well as pleasurable reading materials. In Section 3, some other characteristics of Schoof's expository work will be highlighted. My second finding on that morning, the fact that I could recognize Schoof's mathematical narrative, made me pay conscious attention for the first time to the obvious fact that mathematicians develop their own style. In these pages we will describe René Schoof's style as reflected in some of his expository works.

The 20th century was, until its final decades, an era of “modern mathematics” in a sense quite parallel to “modern art” or “modern architecture” or “modern music.” That is to say, it turned to an analysis of abstraction, it glorified purity and tried to simplify its results until the roots of each idea were manifest.
(David Mumford [12])

If we can recognize a painting by Mondrian or a building by Berlanger, why not a mathematical explanation by Schoof? Just as our eyes have to be trained before we recognize an artist's strokes, our minds have to be trained before we recognize a mathematician's narrative. It is clear that if we have never seen the paintings of Mondrian, reading an article on his style will not enable us to recognize his canvases on the spot; but it will hopefully make us want to see them. Our only aim in these pages will be to awaken in our readers the desire to enjoy Schoof's mathematical writings. With this goal in mind, we have selected three of his expository writings. We will try to illustrate through them both Schoof's personal style of looking at, doing, organizing and explaining mathematics, as well as the cartographic feature of his expositions. Behind

¹Well known examples are the extensive collection of expository papers by Keith Conrad, available online and covering a variety of specific topics in algebraic, analytic, and elementary number theory, or the articles “It's as easy as abc ” [6], a survey of the arithmetic consequences of the abc conjecture, and “Number theory as gadfly” [10], a survey of the unifying consequences for several mathematical fields of the Taniyama–Shimura–Weil conjecture, which cover broader territories of number theory.

our choice stands a story; the concrete pieces that we have chosen could be thought of as the three legs of a tripod on which stands a beautiful story involving René Schoof, Francisco Thaine, and Lawrence Washington that will be told in Section 3.3.

The words “do not disturb my circles” are said to be Archimedes’ last before he was slain by a Roman soldier in the tumult of the pillaging of Syracuse. The timeless tranquil eternity of the not-to-be-disturbed circles in the midst of this account of hurly-burly and death is emblematic of the contrast between mathematics and stories: history, legends, anecdotes and narratives of all sorts thrive on drama, on motion and confusion, while mathematics requires a clarity of thought that, in many instances, comes only after prolonged quiet reflection. At first glance, then, it might seem that mathematics and narrative have little use for each other, but this is not so. As anyone who teaches the subject knows well, the appropriate narrative helps make its substance more comprehensible, while the lack of a narrative frame may render mathematics indigestible or even, at times, downright incomprehensible. [...] Stories play crucial roles in our discovering, creating, explaining and organizing knowledge, and thus mathematics also has great need for narrative, even though its taste for general ideas might make one forget this. (Apostolos Doxiadis and Barry Mazur [2])

2 René Schoof’s mathematical training

In August 1994, a summer school on Fermat’s last theorem took place in *El Escorial* campus of *Universidad Complutense de Madrid*. Organized with the help of René Schoof, the introductory series of lectures were conceived as a whole; the speakers, Ángela Arenas, Pilar Bayer, J.W.S. Cassels, Capi Corrales, Catherine Goldstein, René Schoof, Alf van der Poorten, and Lawrence Washington, based their intervention on the previous ones and would, in turn, be ground for the next ones. Washington closed the course with an explanation of the strategy followed by Andrew Wiles to prove Fermat’s last theorem and Goldstein opened it with a reflection on the different ways to approach the history of mathematics in general, and of Fermat’s last theorem in particular. Her exposition [4] shifted my way of looking at the discipline and has framed much of what follows in these pages. In it, she describes three types of historical narrative of mathematics. The first one would consist of a chronological ordering of all the pertinent results. The second one would be to group these results by families of thought and methods.

The third type of historical narrative is better described by its questions. The following are certainly crucial: What are, at a given time, the social networks or the institutions where the research is done? Who are the mathematicians (teachers, priests, aristocrats, full-time researchers, civil or military engineers, painters, members of a club...)? In which conditions do they live and work on mathematics? Why do they do number theory? Is it usual to invent new results or to transmit them in a new form? Does

one want to understand nature or physical phenomena, count goods, cure, predict, discover pure gems of mathematics for their own sake, in order to celebrate God or the power of the mind? How and where are they trained? How do they learn basic mathematics? What are the basic mathematics of the time? What is basic number theory? Where does one find the problems? When and why do other people find a result important or at least interesting? According to which criteria? Where does one find the mathematical tools which are needed? In the formal training that one has received? Among near collaborators? In recent or very ancient books? What is a solution to a problem? What does one prove? When is it decided that something has to be proved or not? By whom? When is a proof accepted or rejected? When is an explicit construction needed or superfluous? Who (or soon perhaps what...) checks the proofs and the constructions? Is there a codified and rigid procedure to do this? When, where, what is written? For whom? Are mathematics printed, put into practice, taught immediately or with some delay? What is transmitted, to whom and how?

(Catherine Goldstein [4])

Most professional mathematicians are trained along a similar path that includes the postgraduate degree *Doctor of Philosophy* (PhD). Under the guidance of a professor, candidates to a PhD must produce a thesis involving original research. After the initial years, regular courses are complemented with seminars in which students are introduced to research. This emphasis on training for research originated in Germany in the nineteenth century.

In the nineteenth century, German mathematics reached its peak. During this period, under German influence, mathematics (and especially pure mathematics) became a modern scientific discipline. German mathematicians took over from the French as the international leaders. They carried forward the programme of rigorization which had emerged in France after the revolution. [...] Another development, which also originated in the Prussian universities, became significant for the mathematical community. This was the seminar, which provided exercises once a week to complement the normal lecture courses, thereby furnishing an alternative to listening passively to lectures. [...] The first person to apply the seminar model to mathematics was Carl Jacobi. Within the universities, seminars were the only way that students could have scientific contact with their professors, and professors could guide and advise students. The students taking part would have to give a lecture on a topic assigned to them by the professor, and the professor (and to a lesser degree the other participants too) would comment on and criticize the presentation.

(Gert Schubring [21])

René Schoof initiated his studies of mathematics in 1974 at the *Universiteit van Amsterdam*, where he was an assistant from 1976 to 1979. Around 1977 he started attending the national seminar ran by Frans Oort and Gerard van der Geer, attended mostly by

young faculty. Recently published articles would be read;² Schoof recalls having been particularly impressed by Barry Mazur's *Modular curves and the Eisenstein ideal* [9] and thinking that was the type of mathematics that he wanted to do. He graduated in 1979 and became a doctorate student of Hendrik Lenstra, who had just become a professor and did not have the possibility to create a position for him. Thus, Schoof entered the graduate program of the *Universiteit Leiden* under the official supervision of Robert Tijdeman. For four years he worked on his own, studying by himself the type of mathematics that he liked and obtaining a few new results. These were later to become independent chapters in his thesis, e.g. his point-counting algorithm, which he constructed in 1982.³

The problem of calculating the trace of an elliptic curve over a finite field has attracted considerable interest in recent years. There are many good reasons for this. The question is intrinsically compelling, being the first nontrivial case of the natural problem of counting points on a complete projective variety over a finite field, and figures in a variety of contexts, from primality proving to arithmetic algebraic geometry to applications in secure communication. It is also a difficult but rewarding challenge, in that the most successful approaches draw on some surprisingly advanced number theory and suggest new conjectures and results apart from the immediate point-counting problem. It is those number-theoretic considerations that this paper addresses, specifically Schoof's algorithm and a series of improvements using modular curves that have made it practical to compute the trace of a curve over finite fields whose size is measured in googols. [...] Shortly after [14] appeared, but before learning of that paper, I suggested the following approach to computing t . [...] When I showed this to Barry Mazur, he consulted Michael Rabin, who quickly directed me to the paper [14]. It appeared that Schoof had already accomplished what I had set out to do and more.

(Noam D. Elkies [3])

Schoof's contract as an assistant with the *Universiteit Leiden*, which had started in 1980, ended in 1983. With the intervention of Hendrik Lenstra and funded by Don Zagier, he spent the academic year 1983–1984 as a visiting lecturer at the University of Maryland, where Larry Washington took him under his wing, we could say. He returned to the Netherlands in 1984 and within a year he had written his thesis, *Elliptic Curves and Class Groups* [13], which he defended at the *Universiteit van Amsterdam*. His thesis advisor was Hendrik Lenstra, who had also obtained his PhD from the *Universiteit van Amsterdam* with the thesis *Euclidean number fields* [8]. Lenstra's advisor had been Frans Oort.

Johannes G. van der Corput (1890–1975) and Hendrik D. Kloosterman (1900–1968) pioneered the study of number theory in the Netherlands. Both were

²Like most Dutch students of his generation following the STEM direction, Schoof had studied three years of French, three years of German and six years of English in high school.

³During the talk *Counting points on elliptic curves and beyond* that he gave at Microsoft Research in 2007, Schoof himself explained the story of his finding and publishing this algorithm before he had written a thesis. The talk is available at <https://youtu.be/5qCuy2nEYks>.

students of Jan C. Kluyver (1860–1932), who worked in analysis, differential geometry, and –indeed– number theory. Kloosterman also spent some time abroad with famous mathematicians, e.g., G.H. Hardy at Oxford, E. Landau at Göttingen, and E. Hecke at Hamburg. Frans Oort (1935), officially a PhD student of van Est’s, turned to algebraic geometry under the influence of Kloosterman, and was instrumental in shaping the current landscape in algebraic number theory and algebraic geometry. (Klaas Landsman [7])

3 Three examples of René Schoof’s mathematical road maps

3.1 Algebraic number theory

Richard Dedekind defended his habilitation in 1854 at the *Universität Göttingen*, where he remained as a private lecturer until 1894. There, he regularly attended Gustav Lejeune Dirichlet’s lectures on number theory (1856) and studied the works of Ernst Kummer, Niels Henrik Abel and Évariste Galois. In 1863 he edited and published Dirichlet’s *Lectures in number theory*, in which he included two supplements, Supplements X and XI, where he explained his own ideas on number theory and gave a new and modern treatment of Galois theory in terms of field extensions. The book was re-edited in 1871, 1879 and 1893 and in each new edition Dedekind would extend his two supplements. Supplement XI (of which a fifth and more complete version exists in a handwritten manuscript found upon his death in 1916) is considered to be one of the foundations of modern algebraic number theory. In it, Dedekind introduces Gaussian integers, fields, field homomorphisms, number fields, discriminants, rings of algebraic integers (which he calls domains, the name ring being due to Hilbert), ideals, norms of ideals, ideal class groups, class number, proof of the finiteness of the class number, the unit group and proof of Dirichlet’s unit theorem. He also introduces regulators, what is today known as Dedekind’s zeta function of a number field and the Dedekind class number formula; a detailed description can be found in [11]. In [15], Schoof exposes some of the concepts studied by Dedekind, by means of Mordell’s equation $X^3 = Y^2 + d$. The elegant logical structure of Schoof’s exposition translates into the beautiful map of Figure 1.

3.2 Catalan’s conjecture

Je vous prie, Monsieur, de vouloir bien énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n’aie pas encore réussi à le démontrer complètement : d’autres seront peut-être plus heureux : Deux nombres entiers consécutifs, autres que 8 et 9, ne peuvent être des puissances exactes ; autrement dit : l’équation $x^p - y^q = 1$ dans laquelle les inconnues sont entières et positives, n’admet qu’une seule solution.

(Eugène Charles Catalan [1])

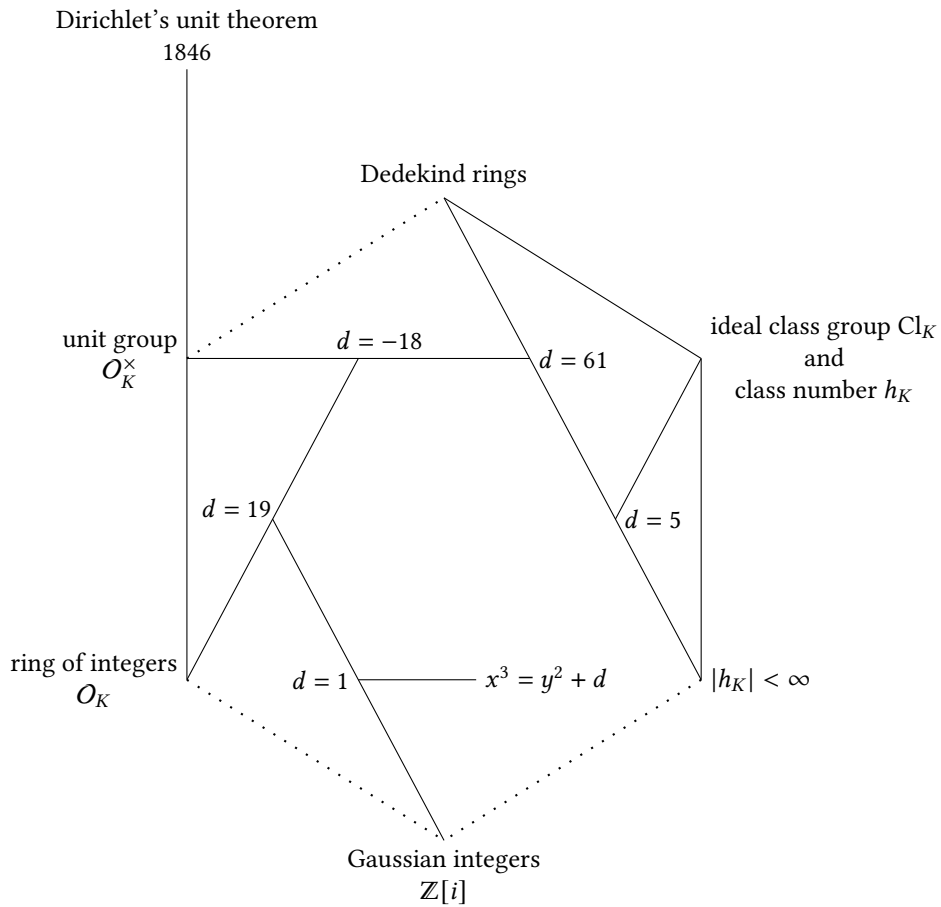


Figure 1: Visualization of René Schoof's road map of Richard Dedekind's hexagon for the number field $K = \mathbb{Q}(\sqrt{-d})$ (1863–1893) associated with the Mordell equation $X^3 = Y^2 + d$ (1914).

In his book [16], René Schoof offers a proof *from scratch* of Catalan's conjecture. As is characteristic of his way of doing, Schoof chooses a point of view that allows him to describe from a common contemporary frame the proofs of the different cases of Catalan's equation constructed through time: Euler (1738) took care of $X^2 = Y^3 + 1$; Lebesgue (1850) dealt with $X^p = Y^2 + 1$ for any exponent $p \geq 2$; Ko Chao (1965) studied $X^2 = Y^q + 1$ for $q \geq 5$; finally, between 2000 and 2006, Preda Mihăilescu proved in four theorems Catalan's conjecture for odd prime exponents. It is also characteristic of Schoof that, when exposing well-known results, he does not always follow the standard approach. For example, he substitutes Euler's proof, based on descent arguments, by the beautiful proof of William McCallum, who dealt with the problem as a student participating in a 1977 honors project at the University of New South Wales; McCallum used π -adic arguments in the field $\mathbb{Q}(\sqrt[p]{2})$, π being the unique prime, up to units, lying above 3 in the ring $\mathbb{Z}[\sqrt[p]{2}]$. A second example is Stickelberger's theorem for $\mathbb{Q}(\zeta_p)$. Schoof chooses Kummer's 1847 beautiful proof which, unlike more standard ones, does not make use of class field theory nor Chebotarev's density theorem.

As has been mentioned, Mihăilescu proved in four theorems Catalan's conjecture for odd prime exponents. Let p, q be odd primes and suppose that x, y are nonzero integers for which $x^p - y^q = 1$.

Mihăilescu I (2000, "the double Wieferich criterion").

We have $p^{q-1} \equiv 1 \pmod{q^2}$ and $q^{p-1} \equiv 1 \pmod{p^2}$.

Mihăilescu II (2002). If $p, q > 5$, then $p \equiv 1 \pmod{q}$ or $q \equiv 1 \pmod{p}$.

Mihăilescu III (2003). If $p, q > 5$, then $p < 4q^2$ and $q < 4p^2$.

Mihăilescu IV (2006). If $p \leq 41$ or $q \leq 41$, Catalan's equation has no solution in non-zero integers.

The first three theorems of Mihăilescu suffice to prove Catalan's conjecture when $p, q > 5$. The last theorem takes care of the smaller values of the primes. Mihăilescu weaves in his arguments several fundamental threads spun along the last two centuries by number theorists. Schoof carefully unweaves them, rephrases them in terms of a common contemporary point of view and then elegantly weaves them back together. After summarizing Mihăilescu's approach in Schoof's terms, we will describe, using three steps for each theorem, the main threads unweaved by Schoof in Mihăilescu's proofs. Next, we will give an example of Schoof's rephrasing of arguments into a common narrative. Finally, we will translate the logical structure of Schoof's exposition into a map to travel the proof of Catalan's conjecture. We will not reproduce any of the beautiful and often deep arguments in the exposition of Schoof; our only aim will be to illustrate his style of doing mathematics, and we believe that the best way to do so is by keeping it simple. To use a metaphor reminiscent of the conference René 25, which took place at the *Université de la Polynésie française* in August 2025, we will just snorkel from the surface of Schoof's exposition of Catalan's conjecture. Readers wanting to go deeper are invited to read his wonderful book [16].

A first draft of this book was written in August 2003. It is based on two sets of lecture notes by Yuri Bilu. In the following years, the draft was used in student seminars in Rome, in the island of Menorca, and in Regensburg. With the benefit of these experiences, a new version was written. It is the basis of this book. (René Schoof [16])

A solution to Catalan's equation leads to the factorization $y^q = \prod_{k=0}^{p-1} (x - \zeta_p^k)$ in the cyclotomic field $\mathbb{Q}(\zeta_p)$, with ζ_p a primitive root of unity. Let π be the only prime ideal above p in the ring of integers $\mathbb{Z}[\zeta_p]$, $G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $\iota \in G$ complex conjugation. The element $x - \zeta_p$ lies in the obstruction group

$$H = \{ \alpha \in \mathbb{Q}(\zeta_p)^\times \mid \text{ord}_\varphi(\alpha) \equiv 0 \pmod q \text{ for each prime } \varphi \neq \pi \} / \mathbb{Q}(\zeta_p)^{\times q}$$

which is a $\mathbb{F}_q[G]$ -module. It is precisely by translating the different arguments weaved in Mihăilescu's four proofs in terms of the group H , studied in [16, Chapter 7], and some of its subgroups, that Schoof is able to present them all from a common contemporary point of view.

Structure of Schoof's proof of Mihăilescu IV [16, Chapters 7 & 8].

Assume $x^p - y^q = 1$ where $x, y \in \mathbb{Z}$ satisfy $xy \neq 0$ and p, q are primes such that $p \leq 41$ or $q \leq 41$.

1. Using π -adic arguments, it is proved that if p, q are odd primes then the element $(x - \zeta_p)^{1-\iota}$ is a nontrivial element in the obstruction group H .
2. It is known (Kummer) that the ideal class group Cl_p of $\mathbb{Q}(\zeta_p)$ splits in a natural way in two parts, the *plus class group* Cl_p^+ and the *minus class group* Cl_p^- , with respective orders h_p^+ and h_p^- . Mihăilescu proves that if p, q are odd primes such that q does not divide h_p^- or p does not divide h_q^- , then Catalan's equation $x^p - y^q = 1$ has no solutions $x, y \in \mathbb{Z}$.
3. We may assume $p < q$. Around 1850, Kummer computed the value of h_p^- for $p < 100$ [16, Table 7.1]. Inspection of these values shows that, when $p \leq 41$, the prime divisors of h_p^- are less than or equal to p . Thus, q , being larger than p , cannot divide h_p^- . Thus, Step 2 implies that Catalan's equation has no integer solutions and Mihăilescu IV is proved. $\square$

Structure of Schoof's proof of Mihăilescu I [16, Chapters 7, 9 & 10].

Assume $x^p - y^q = 1$ where $x, y \in \mathbb{Z}$ satisfy $xy \neq 0$ and p, q are odd primes.

1. In 1960, J.W.S. Cassels established that, under the above hypothesis, q divides x and p divides y . The main ingredient in the proof of Cassels' theorem is the Runge method for finding solutions to certain Diophantine equations. As a corollary to this theorem, we have the three facts: $x \equiv 1 \pmod{p^{q-1}}$ and $y \equiv 0 \pmod p$; $x \equiv 0 \pmod q$ and $y \equiv -1 \pmod{q^{p-1}}$; $|x|, |y| \geq \max(p^{q-1} - 1, q^{p-1} - 1)$.
2. Properties of the cyclotomic field $\mathbb{Q}(\zeta_p)$ are used to prove that the ideal $I \subset \mathbb{Z}[G]$, product of the Stiklberger's ideal and $1 - \iota$, annihilates the group H . This fact is a key ingredient in the proof that $q^2 \mid x$ and $p^2 \mid y$.

3. Using Fermat's little theorem and the results of the previous two steps, Mihăilescu I is proved. $\square$

Schoof concludes his exposition of Mihăilescu I by rephrasing the theorem in terms of the group H : if $x, y \in \mathbb{Z}$ are a solution to Catalan's equation with p, q odd primes, then the image of $x - \zeta_p$ in H is contained in its subgroup $S = \{\alpha \in H : \alpha \text{ is a } q\text{-adic } q^{\text{th}} \text{ power}\}$, called a *Selmer group*.⁴

Structure of Schoof's proof of Mihăilescu III [16, Chapters 6, 7 & 11].

Assume $x^p - y^q = 1$ where $x, y \in \mathbb{Z}$ satisfy $xy \neq 0$ and $p, q \geq 5$ are primes.

1. There is an injective homomorphism

$$\{\theta \in \mathbb{Z}[G] : (x - \zeta_p)^\theta = \alpha^q, \text{ for some } \alpha \in \mathbb{Q}(\zeta_p)^\times\} \longrightarrow \mathbb{Q}(\zeta_p)^\times$$

between the $\mathbb{Z}[G]$ -annihilator of $x - \zeta_p$ in H and $\mathbb{Q}(\zeta_p)^\times$, given by $\theta \mapsto \alpha$.

2. If $|x| \geq 2$ and $\theta \in (1 - \iota) \subset \mathbb{Z}[G]$ is in the $\mathbb{Z}[G]$ -annihilator of $x - \zeta_p$ in H , with associated element α via the map defined in the previous step, then for every embedding $\phi : \mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C}$ the number $\phi(\alpha)$ is contained in the unit circle and there exists a q^{th} root of unity ξ with $|\phi(\alpha) - \xi| \leq \frac{\|\theta\|}{q(|x|-1)}$.
3. We may assume $q > 4p^2$. Since, as proved in Mihăilescu I, the ideal I product of the Stikelberger's ideal and $1 - \iota$, annihilates the group H , Step 2 applies to all $\theta \in I$. This is used to prove that there exists a nonzero element $\theta \in I$ with $\|\theta\| \leq \frac{3q}{p-1}$ such that $(x - \zeta_p)^\theta = \alpha^q$, for some $\alpha \in \mathbb{Q}(\zeta)^\times$, and

$$(|x| + 1)^{-\frac{p-1}{2q}\|\theta\|} \leq |N(\alpha) - 1| \leq \frac{2^{p-1}}{q^2} \left(\frac{\|\theta\|}{|x| - 1} \right)^2.$$

Since $p \geq 5$ and, as a consequence of Cassels' theorem, $|x| > q^{p-1}$, these inequalities together lead to $q < 4$, which contradicts $q \geq 5$. Thus $q > 4p^2$ as wanted and Mihăilescu III is proved. $\square$

Structure of Schoof's proof of Mihăilescu II [16, Chapters 12 & 14].

Assume $x^p - y^q = 1$ where $x, y \in \mathbb{Z}$ satisfy $xy \neq 0$ and $p, q > 5$ are primes. Suppose that $p \not\equiv 1 \pmod{q}$ and $q \not\equiv 1 \pmod{p}$. We will work within $S^+ = \{(1 + \iota)\alpha : \alpha \in S\} \subset S \subset H$.

1. We associate to the solution of Catalan's equation a certain power series in $\mathbb{Q}(\zeta_p)[[T]]$. The Runge method is used to show that properties of this series imply that the $\mathbb{F}_q[G^+]$ -annihilator of the element $(x - \zeta_p)^{1+\iota} \in S^+$ is trivial.
2. Thaine's theorem (Section 3.3) is used to show that S^+ has a non-zero annihilator.
3. The results of the previous two steps combined lead to a contradiction. Thus $p \equiv 1 \pmod{q}$ or $q \equiv 1 \pmod{p}$ and Mihăilescu II is proved. $\square$

See Figure 2.

⁴Once H is interpreted as a flat cohomology group, S can be view as the kernel of a global-to-local map, closely aligned with the definition of Selmer groups for elliptic curves.

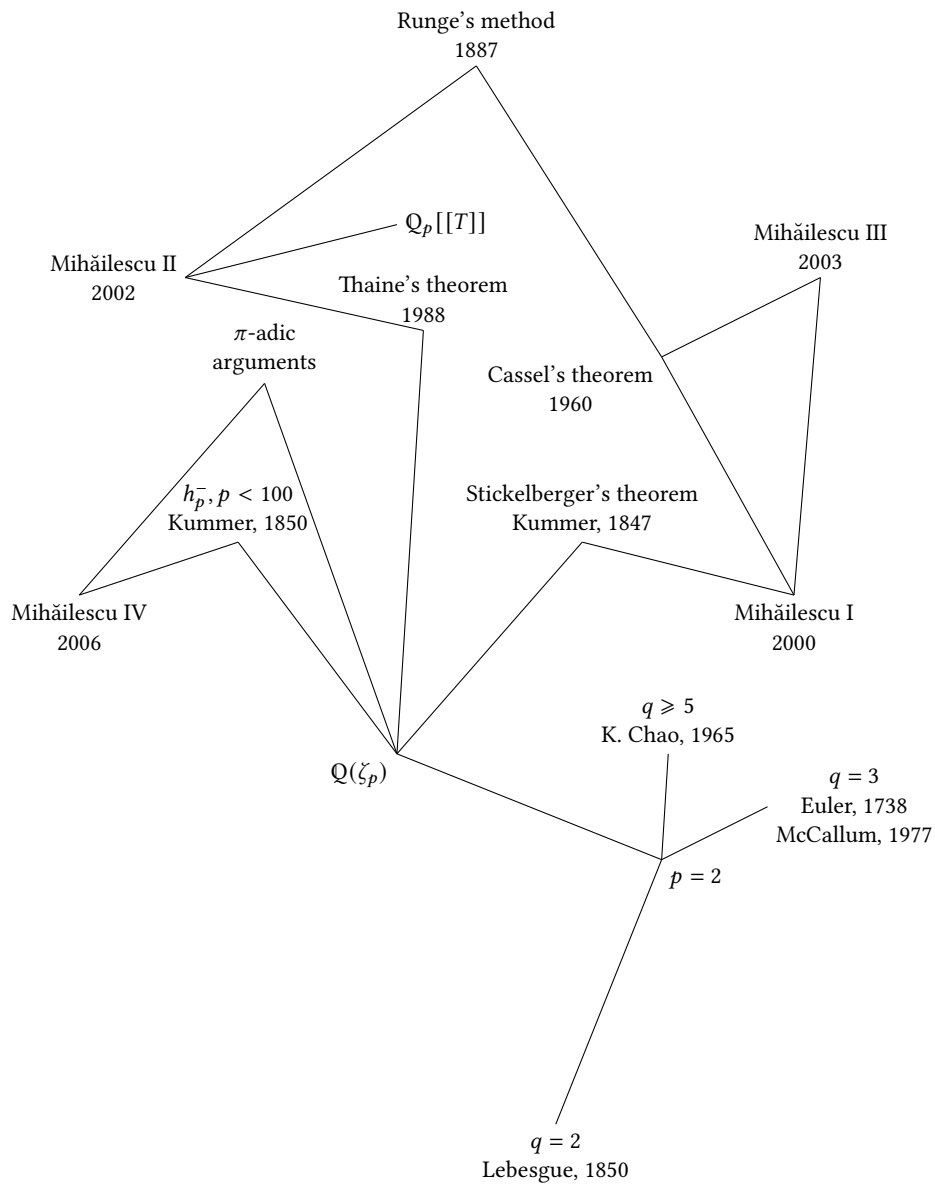


Figure 2: Visualization of René Schoof's road map for Preda Mihăilescu's proof of Catalan's conjecture (2002–2006).

A shallow dive in Schoof's style. An illustrative and especially beautiful example of Schoof's style is the logical structure of his exposition of the second step in the proof of Mihăilescu I: to show that, if $x^p - y^q = 1$ with $x, y \in \mathbb{Z}$, $xy \neq 0$, and p, q odd primes, then $q^2 \mid x$ and $p^2 \mid y$.

Sketch of the structure of Step 2 in Schoof's proof of Mihăilescu I [16, Chapters 7, 9 & 10]. The argument has two parts. In the first one, it is showed that there are elements in $\mathbb{Z}[G]$ which annihilate the elements of the obstruction group H . An argument by contradiction gives the required result in the second part.

For the first part, let $E_p = \mathbb{Z}[\zeta_p, 1/p]^\times$ be the group of p -units in $\mathbb{Q}(\zeta_p)$ and $\text{Cl}_p[q]$ the subgroup of its ideal class group Cl_p formed by the ideal classes c such that $c^q = \mathbb{Z}[\zeta_p]$. There is an exact sequence of $\mathbb{F}_q$ -modules

$$0 \longrightarrow E_p/E_p^q \longrightarrow H \xrightarrow{\Phi} \text{Cl}_p[q] \longrightarrow 0.$$

Consequently, in order to find elements $\theta \in \mathbb{Z}[G]$ which annihilate the elements of H it suffices to find elements which annihilate E_p/E_p^q and elements which annihilate $\text{Cl}_p[q]$. It turns out that E_p/E_p^q is invariant under the action of complex conjugation ι , and so $1 - \iota$ annihilates E_p/E_p^q . On the other hand, the elements of the Stickelberger's ideal annihilate the class group, and thus its subgroup $\text{Cl}_p[q]$. Schoof presents Kummer's beautiful 1847 proof of this fact, which he exposes in terms that any one with a basic background in algebraic number theory can understand. We conclude that the ideal I product of the Stickelberger's ideal and $1 - \iota$ annihilate the group H .

For the second part, suppose that $x \not\equiv 0 \pmod{q^2}$ (or, by symmetry, $y \not\equiv 0 \pmod{p^2}$). Mihăilescu proved that this would imply that all the elements in the ideal I would have their coefficients divisible by q . But the element

$$-\sum_{1 \leq a \leq \frac{p-1}{2}} \sigma_a^{-1} + \sum_{\frac{p+1}{2} \leq a \leq p-1} \sigma_a^{-1} \in I,$$

with $\sigma_a(\zeta_p) = \zeta_p^a$, for example, does not satisfy this condition. Consequently $x \equiv 0 \pmod{q^2}$ and $y \equiv 0 \pmod{p^2}$. $\square$

The neat little book under review gives a complete account of Mihăilescu's proof including most of the background material. The key ingredients are Runge's method, explained here in terms of the theory of algebraic curves, and the theory of cyclotomic fields, including the theory of the Stickelberger ideal and a crucial theorem of Thaine. The latter is the hardest –and most recent– of the prerequisites, and is relegated to the final chapter. Catalan's conjecture is very readable, direct, and full of insight. It manages to completely explain a significant recent result “from scratch” in a mere 120 pages, quite an achievement these days. It makes for delightful reading for any number theorist, but it would also be an excellent way to learn some algebraic number theory. One could easily build an undergraduate seminar around it; I'm sure students would enjoy it and learn a lot. It's an excellent book.

(Fernando Q. Gouvêa [5])

3.3 Thaine's theorem

Mi tesis de doctorado era sobre aritmética de los cuerpos ciclotómicos. Fui contratado por la Universidad de Brasilia donde conseguí una beca para estudiar (¡suerte mía!) con Paulo Ribenboim que fue orientador de mi orientador Tenkasi Viswanathan. Ribenboim (¡suerte mía!) me encaminó a estudiar con Lawrence Washington que (¡suerte mía!) me presentó a René Schoof. (Francisco Thaine [23])

My doctoral thesis was on the arithmetic of cyclotomic fields. I was hired by the University of Brasilia where I obtained a scholarship to study (lucky me!) with Paul Ribenboim who was the advisor of my advisor Tenkasi Viswanathan. Ribenboim (lucky me!) guided me towards studying with Lawrence Washington who (lucky me!) introduced me to René Schoof.

In 1994 Francisco Thaine was invited by Jesús Gómez de Ayala, from *Universidad del País Vasco* in Bilbao, to attend the summer school on Fermat's last theorem that took place in *El Escorial* that August. During one of the conversations at lunch time, Washington, Schoof and Thaine recalled together their one-day meeting in Maryland in 1983. During the celebration of René 25, also in August and also at lunch time, Larry Washington recalled the story. Francisco Thaine had spent the academic year 1982–1983 at the University of Maryland, where he had attended a course on class field theory taught by Lawrence Washington, and René Schoof arrived there just as Thaine was leaving. They overlapped for one day, during which Thaine and Washington explained to Schoof the conjecture that Thaine was working on and a step in it that remained to be solved. Schoof worked on it during the following weeks and solved it. As Thaine himself explains in the introduction to [24], the step, which fits into a larger picture over which he had been discussing with Washington during his stay at Maryland, became part of what is now known as Thaine's theorem.

I didn't hear much more from Francisco until summer of 1986, when he sent René and me a manuscript that gave a Stickelberger-type result. Fortunately, I was at MSRI during 1986–1987 so I had time to study the paper carefully. Finally, I was able to rewrite the proof in a way that convinced me it was completely correct. That afternoon, I went down to afternoon tea at MSRI and was talking with Karl Rubin and David Rohrlich, when Karl noticed that Dave was carrying an envelope with a yellow and green border. Recognizing those as Brazil's colors, Karl asked who was the person he knew in Brazil. David answered and then turned to me and asked didn't I also know someone in Brazil. I said yes it was Francisco Thaine and he'd just proved a really nice result. Karl's eyes lit up. This was exactly the type of technique he needed for proving Sha is finite. I showed him Thaine's manuscript and my reworking, and a few days later Karl announced his proof that CM elliptic curves of rank 0 have finite Sha. I like to think this had further effects: Andrew Wiles had been trying to prove the finiteness by another method, namely, by proving a "main conjecture" for elliptic

curves. When Karl proved the result, Andrew looked for something else to work on. The rest of the story is well-known. So Francisco, whose goal, as for many of us, was to prove FLT, actually played a role in getting FLT proved!
(Larry Washington [26])

Theorem (Thaine's theorem [24]). *Let $K \neq \mathbb{Q}$ be a real abelian number field. Let E be the group of units of the ring of integers of K , $C \subset E$ the group of circular units, A the ideal class group of K and Δ the Galois group of $K/\mathbb{Q}$. Let $W = E/C$ and, for p prime, let $(A)_p$ and $(W)_p$ be the p -Sylow subgroups of A and W . If $\theta \in \mathbb{Z}[\Delta]$ annihilates $(W)_p$, then 2θ annihilates $(A)_p$.*

Proof in the setting of Catalan's conjecture [16, Chapter 16].

Let p be an odd prime. Let ζ_p denote a primitive p^{th} root of unity and $\zeta_p^+ = \zeta_p + \zeta_p^{-1}$. We will work in the cyclotomic field $\mathbb{Q}(\zeta_p)$ and we set the following notation. Set $G = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and denote by ι the automorphism that induces complex conjugation; let $F = \mathbb{Q}(\zeta_p^+)$ and $G^+ = \text{Gal}(F/\mathbb{Q}) = G/\langle \iota \rangle$; denote by E the group of p -units in $\mathbb{Q}(\zeta_p)$, by $C \subset E$ the subgroup of cyclotomic p -units, by E^+ the subgroup of ι -invariant p -units, and by C^+ the subgroup of ι -invariant cyclotomic p -units; let Cl be the ideal class group of $\mathbb{Q}[\zeta]$ and Cl^+ the ideal class group of F .

There is an isomorphism of $\mathbb{Z}[G]$ -modules $E^+/C^+ \xrightarrow{\cong} E/C$. It was already known to Kummer that $|E/C|$ is of finite order $|E/C| = |E^+/C^+| = |\text{Cl}^+|$. It is also known that, in general, the groups E/C and Cl^+ are not isomorphic [25, page 146]. Thaine's theorem establishes a relation between them:

If q prime, $q \neq p$, $p \not\equiv 1 \pmod{q}$, then the $\mathbb{Z}[G^+]$ -annihilator of the q -part of E/C also annihilates the q -part of Cl^+ .

Schoof's statement of Thaine's theorem is as follows:

Let p and q be distinct odd primes with q not dividing $p - 1$. Let G^+ be the Galois group of $\mathbb{Q}(\zeta_p^+)$ over $\mathbb{Q}$. If $\theta \in \mathbb{Z}[G^+]$ annihilates E/CE^q then it also annihilates $\text{Cl}^+/\text{Cl}^{+q}$.

His beautiful proof of this statement involves three steps. See Figure 3.

With the notation introduced above, let p and q be distinct odd primes with q not dividing $p - 1$. There are isomorphisms

$$E^+/E^{+q} \xrightarrow{\cong} E/E^q \quad \text{and} \quad E^+/C^+E^{+q} \xrightarrow{\cong} E/CE^q$$

between $\mathbb{F}_q[G^+]$ -modules of rank 1. Let $u \in E^+$ whose class is a generator of them all.

We have: an element $\theta \in \mathbb{Z}[G^+]$ such that $u^\theta = \gamma v^q$ for some $\gamma \in C^+$ and $v \in E^+$. We want: given any $c \in \text{Cl}^+$ produce an ideal $I \subset F$ such that $[I] = c$ and $[I^\theta] \in \text{Cl}^{+q}$.

1. We want to produce a prime ideal $\mathfrak{J}$ of F of degree 1 with three properties:

- $[\mathfrak{J}] = c$ in $\text{Cl}^+/\text{Cl}^{+q}$;
- $\mathfrak{J}$ lies over a prime number ℓ that is congruent to 1 mod pq ;

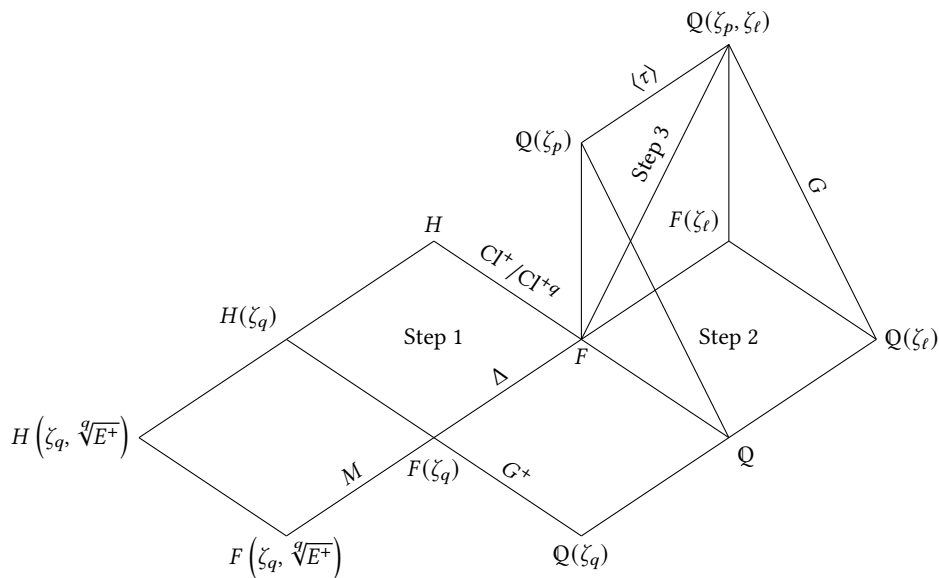


Figure 3: Visualization of René Schoof's road map for the proof of Francisco Thaine's theorem (1988) in the setting of Catalan's conjecture.

- $E^+/E^{+q} \xrightarrow{\cong} (O_F/\ell O_F)^\times / (O_F/\ell O_F)^{\times q}$ is an isomorphism of $\mathbb{F}_q[G^+]$ -modules of rank 1.

To do so, let $H(F)$ be the Hilbert class field of F with $\text{Gal}(H(F)/F) \cong \text{Cl}^+$, $H \subset H(F)$ be such that $\text{Gal}(H) \simeq \text{Cl}^+/\text{Cl}^{+q}$ and $\Delta = \text{Gal}(F(\zeta_q)/F)$. We consider the lattice of fields displayed in Figure 4 where we have the isomorphisms

$$\begin{aligned} \text{Gal}\left(F(\zeta_q, \sqrt[q]{E^+})/F(\zeta_q)\right) &\xrightarrow{\cong} \text{Hom}(E^+/E^{+q}, \mu_q) = M, \\ \text{Gal}\left(H(\zeta_p, \zeta_q, \sqrt[q]{E^+})/F(\zeta_q)\right) &\xrightarrow{\cong} \text{Cl}^+/\text{Cl}^{+q} \times M \times \langle \iota \rangle. \end{aligned}$$

If m is a generator of M , by Chebotarev's density theorem there exists a prime ideal $\mathcal{L}$ of $\mathbb{F}_p(\zeta_q)$ of degree 1 such that its Frobenius element is (c, m, id) . We take for $\mathfrak{J}$ the prime ideal of F over which $\mathcal{L}$ lies.

2. The existence of the prime ideal $\mathfrak{J}$ of F allows us to work in the lattice of fields of Figure 5 with $\mathfrak{J}$ prime above ℓ in F , $\mathcal{L}$ prime above ℓ in $Q(\zeta_p, \zeta_l)$ and $\text{Gal}(Q(\zeta_p, \zeta_l)/Q(\zeta_p)) = \langle \tau \rangle$ with $\tau(\zeta_l) = \zeta_l^s$. In this setting, we construct a unit $\varepsilon \in Q(\zeta_p, \zeta_l)^\times$ with $\varepsilon \equiv \gamma \pmod{\zeta_l - 1}$ and $N_{Q(\zeta_p, \zeta_l)/Q(\zeta_p)}(\varepsilon) = 1$. Hilbert's Theorem 90 tells us that $\varepsilon = \alpha/\tau(\alpha)$ for some $\alpha \in Q(\zeta_p, \zeta_l)^\times$. The factorization of the ideal generated by α is key in Thaine's proof: $(\alpha) = J \prod_{\sigma \in G} \sigma(\mathcal{L})^{r_\sigma}$, with J a $Q(\zeta_p)$ -ideal prime to ℓ , $r_\sigma \in \mathbb{Z}$.

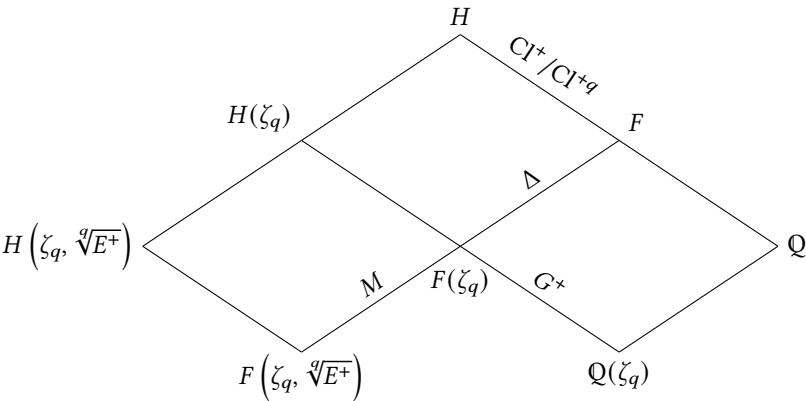


Figure 4: Lattice of fields involved in Step 1.

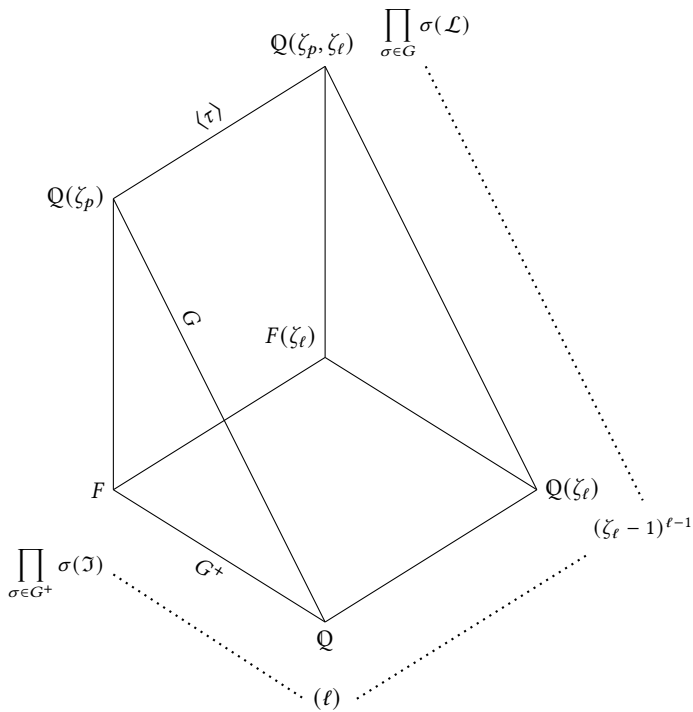


Figure 5: Lattice of fields involved in Step 2.

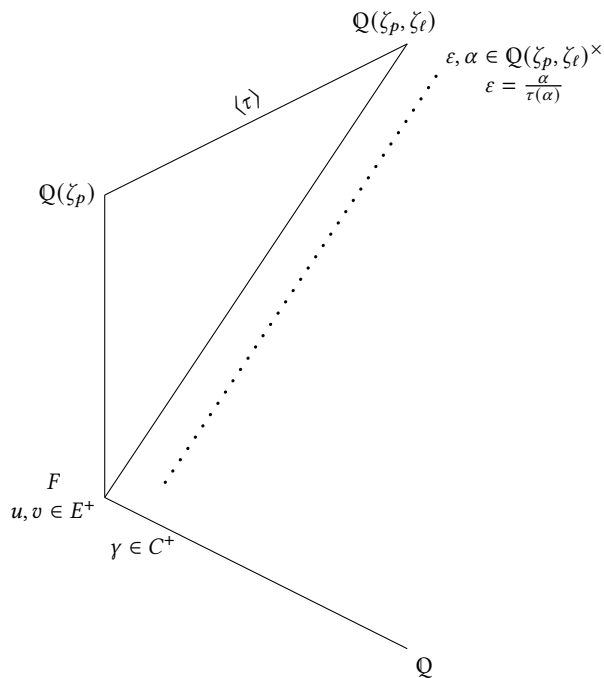


Figure 6: Lattice of fields involved in Step 3.

3. We have the situation of Figure 6.

On the one hand, $(\alpha) = J \prod_{\sigma \in G} \sigma(\mathcal{L})^{r_\sigma}$, which implies that

$$\left(N_{Q(\zeta_p, \zeta_\ell)/F}(\alpha) \right) = J'^{\ell-1} \prod_{\sigma \in G^+} \sigma(\mathfrak{J})^{r_\sigma}, J' = \left(N_{Q(\zeta_p, \zeta_\ell)/F}(J) \right)$$

and so $\sum_{\sigma \in G^+} r_\sigma \sigma$ annihilates $[\mathfrak{J}] = c$ in $\text{Cl}^+/\text{Cl}^{+q}$.

On the other hand, $(\alpha) = J \prod_{\sigma \in G} \sigma(\mathcal{L})^{r_\sigma}$ implies that $\gamma \equiv s^{r_\sigma} \pmod{\sigma(\mathfrak{J})}$ for all $\sigma \in G$. Consequently, $\gamma = \bar{u}^{\sum_{\sigma \in G^+} r_\sigma \sigma}$ for a suitable generator $\bar{u}$ of

$$\prod_{\sigma \in G^+} k_{\sigma(\mathfrak{J})}^\times / k_{\sigma(\mathfrak{J})}^{\times q} \cong (O_F / \ell O_F)^\times / (O_F / \ell O_F)^{\times q} \cong E^+ / E^{+q}$$

and so $u^\theta = \gamma = u^\eta \sum_{\sigma \in G^+} r_\sigma \sigma$ in $(O_F / \ell O_F)^\times / (O_F / \ell O_F)^{\times q}$ with η a unit in $\mathbb{F}_q[G^+]$, and $\theta = \eta \sum_{\sigma \in G^+} r_\sigma \sigma$ in $\mathbb{F}_q[G^+]$. It follows that θ annihilates c in $\text{Cl}^+/\text{Cl}^{+q}$. $\square$

Acknowledgements

I would like to thank Francisco Thaine and Lawrence Washington for sharing with me the story told in Section 3.3. I would also like to thank Eva Bayer, Valerio Talamanca, Francisco Thaine and Lawrence Washington for their comments to earlier versions of these pages. And I especially thank Mariana Alcalde for the beautiful images that she produced out of my hand-drawn road maps.

These maps are abstract pieces made for René Schoof. On the one hand, Schoof taught me how useful it is to work with Hasse diagrams for number fields, of which the last four maps above are examples. On the other hand, in June 2018 I travelled by car with him from downtown NYC to Logan Airport in Boston. Unfortunately the rented car had no road map in it and we both had European connections in our portable telephones. For several hours we navigated our way through the states of Connecticut and Massachussets driving from Starbucks Cafe to Starbucks Cafe, using their WiFi network and designing our trip as if it was a patchwork. Tourism was not a possibility in those conditions and I finally decided to buy a road map. We had to visit several gas stations before we found one where they were sold. Since we had plenty of time to kill, Schoof was happy to join me in the quest, not without expressing several times how unnecessary he found road maps once portable phones provide us with navigations tools. Each time, I would think to myself how odd it was that one of the best mathematics map makers that I knew of would be so reluctant to use one himself as soon as he was in a non mathematical territory. I have since wanted to explain to Schoof what a good map maker he is. This special volume that the *Polynesian Journal of Mathematics* is dedicating to Schoof's mathematics has given me the opportunity.

References

- [1] Eugène Charles Catalan. Note extraite d'une lettre adressée à l'éditeur. *Journal für die reine und angewandte Mathematik*, 27:192, 1844.
- [2] Apostolos Doxiadis and Barry Mazur. Introduction. In *Circles Disturbed: The Interplay of Mathematics and Narrative*, pages VII–XXII. Princeton University Press, 2012. ISBN: 9780691149042.
- [3] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, 1998. ISBN: 9780821808801.
- [4] Catherine Goldstein. Fermat, number theory and history. In *Cuatrocientos años de matemáticas en torno al último teorema de Fermat*, pages 1–22. Universidad Complutense de Madrid, 1999. ISBN: 9788489784383.
- [5] Fernando Q. Gouvêa. Review of René Schoof's book *Catalan's conjecture* (Springer, 2008). Mathematical Association of America, 2009. <https://old.maa.org/press/maa-reviews/catalans-conjecture>

- [6] Andrew Granville and Thomas J. Tucker. It's as easy as *abc*. *Notices of the AMS*, 49(10):1224–1231, 2002.
- [7] Klaas Landsman. The Dutch mathematical landscape. In *NWO cluster evaluation booklet*, pages 1–6. Nederlandse Organisatie voor Wetenschappelijk Onderzoek, 2010.
- [8] Hendrik W. Lenstra, jr. *Euclidische getallenlichamen*. Proefschrift, Universiteit van Amsterdam, 1977.
- [9] Barry Mazur. Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'IHÉS*, 47:33–186, 1977. DOI: 10.1007/BF02684339.
- [10] Barry Mazur. Number theory as gadfly. *The American Mathematical Monthly*, 98(7):593–610, 1991.
- [11] Stefan Müller-Stach. *Richard Dedekind*. Birkhauser, 2017.
- [12] David Mumford. A foreword for non-mathematicians. In *The Unreal Life of Oscar Zariski*, pages XIII–XXII. Academic Press, 1991.
- [13] René Schoof. *Elliptic curves and class groups*. Proefschrift, Universiteit van Amsterdam, 1985.
- [14] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p . *Mathematics of Computation*, 44(170):483–494, 1985. DOI: 10.1090/S0025-5718-1985-0777280-6.
- [15] René Schoof. Algebraic number theory. In *Cuatrocientos años de matemáticas en torno al último teorema de Fermat*, pages 23–32. Universidad Complutense de Madrid, 1999. ISBN: 9788489784383.
- [16] René Schoof. *Catalan's conjecture*. Springer, 2008. ISBN: 9781848001855.
- [17] René Schoof. Computing Arakelov class groups. In *Algorithmic Number Theory*, Volume 44 of *MSRI Publications*, pages 447–495. Cambridge University Press, 2008. ISBN: 9780521808545.
- [18] René Schoof. Four primality testing algorithms. In *Algorithmic Number Theory*, Volume 44 of *MSRI Publications*, pages 101–126. Cambridge University Press, 2008. ISBN: 9780521808545.
- [19] René Schoof. The discrete logarithm problem. In *Open Problems in Mathematics*, pages 403–416. Springer, 2016. ISBN: 9783319321608.
- [20] René Schoof. Heights and principal ideals of certain cyclotomic fields. In *Class Groups of Number Fields and Related Topics*, pages 89–96. Springer, 2020. ISBN: 9789811515149.

-
- [21] Gert Schubring. The German mathematical community. In *Möbius and his band*, pages 21–33. Oxford University Press, 1993. ISBN: 9780198539698.
- [22] Gert Schubring. Changing cultural and epistemological views on mathematics and different institutional contexts in nineteenth-century Europe. In *L'Europe mathématique: histoires, mythes, identités*, pages 363–388. Éditions de la Maison des sciences de l'homme, 1996. ISBN: 9782735106851.
- [23] Francisco Thaine. Private correspondence. October 2025.
- [24] Francisco Thaine. On the ideal class group of real abelian number fields. *Annals of Mathematics*, 128(1):1–18, 1988. DOI: 10.2307/1971460.
- [25] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Volume 83 of *Graduate Texts in Mathematics*. Springer, 1997. ISBN: 9780387947624.
- [26] Lawrence C. Washington. Private correspondence. September 2025.