Annals of Formalized Mathematics
Volume **1** (2025), 103–132
DOI: https://doi.org/10.46298/afm.14586

A complete formalization of Fermat's Last Theorem for regular primes in Lean

Alex J. Best, Christopher Birkbeck, Riccardo Brasca, Eric Rodriguez Boidi, Ruben Van de Velde, Andrew Yang

Abstract. We formalize a complete proof of the regular case of Fermat's Last Theorem in the LEAN4 theorem prover. Our formalization includes a proof of Kummer's lemma, which is the main obstruction to Fermat's Last Theorem for regular primes. Rather than following the modern proof of Kummer's lemma via class field theory, we prove it by using Hilbert's Theorems 90–94 in a way that is more amenable to formalization.

MSC 2020: 68V20, 11D41, 11R18
Keywords: Formalization, mathlib, lean, Fermat's Last Theorem

Contact information:
A. Best: alexjbest@gmail.com
C. Birkbeck: University of East Anglia. c.birkbeck@uea.ac.uk
R. Brasca: Université Paris Cité and Sorbonne Université, CNRS, IMJ-PRG. riccardo.brasca@imj-prg.fr
E. Rodriguez Boidi: ericrboidi@gmail.com
R. Van de Velde: ruben.vandevelde@gmail.com
A. Yang: a.yang24@imperial.ac.uk

Received: October 17, 2024
Final form: June 14, 2025
Accepted: July 2, 2025

1 Introduction

For $x, y, z \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $n > 2$, Fermat's Last Theorem (FLT) is the result that there are no solutions to

$$x^n + y^n = z^n$$

with x, y and z all different from 0. This apparently easy result has been stated by Pierre de Fermat around 1637, but the first full proof, by Andrew Wiles and Richard Taylor, only appeared in 1995 in the two papers [Wil95; TW95]. The quest for a proof of FLT has a long history of driving the development of new mathematics and this has continued now as mathematicians and computer scientists look to formalize mathematics. The importance of FLT lies not in the theorem itself (as number theory is full of seemingly easy equations that turn out to be extremely difficult to solve), but in the theories that have been developed to solve it. Indeed, attempting to prove FLT played a major role in the development of algebraic number theory.

Almost every mathematical statement and definition will be accompanied by a link directly to the source code for the corresponding statement in MATHLIB or in FLT-REGULAR. To keep the links usable, they are all to a fixed commit of the master branch (the most recent one at the time of writing).

A routine argument shows that it is enough to prove FLT in the case where the exponent is equal to 4 or it is a prime number $p \neq 2$. The case $n = 4$, proved by Fermat himself, is not completely obvious but was already in MATHLIB at the beginning of our project, see `fermatLastTheoremFour`. In what follows we will describe the formalization (in the LEAN4 theorem prover) of FLT in the special case where the exponent p is what is known as a regular prime. That is, p is a prime number (different from 2) that does not divide the class number of the p-th cyclotomic extension $\mathbb{Q}(e^{\frac{2\pi i}{p}})/\mathbb{Q}$. This case is significantly simpler than the full version and it is amenable to formalization given the current state of our formalized libraries, such as MATHLIB [mat20].[1] There are several reasons for wanting to formalize the regular case. Firstly, it is a stress test of MATHLIB: even though the tools we need here are much more basic than those required for the full proof, by formalizing this case we have extensively improved the number theory library, finding various issues with MATHLIB's original implementation. As a result of this work, those issues have now been addressed. Secondly, many of the tools required are of independent interest, such as discriminants, cyclotomic fields, ramification results, etc., all of which were originally formalized as a part of this work.

[1] A partial formalization of the full proof is a work in progress by Kevin Buzzard, and it will likely take several years to complete.

Having FLT-REGULAR as our goal allowed us to develop these theories in a cohesive manner. Lastly, this represents the first formalization of a non-trivial family of cases of FLT (a family that is conjecturally infinite).

In the previous work [Bes+23] of (some of) the authors, we formalized the following first step towards proving FLT in the regular case:

Theorem 1.1 (Case 1)**.** *Let p be an odd regular prime. Then $x^p + y^p = z^p$ has no solutions with $x, y, z \in \mathbb{Z}$ and $\gcd(xyz, p) = 1$.*

Here we will be concerned with the full proof (of the regular case), which replaces the condition that $\gcd(xyz, p) = 1$ with $xyz \neq 0$. Specifically we will prove what is known as the second case, where the main difficulty is the need for Kummer's Lemma, which states that:

Lemma 1.2. *Let p be an odd regular prime and let $\zeta \in \mathbb{C}$ be a primitive p-th root of unity. If $u \in \mathbb{Z}[\zeta]^\times$ is a unit such that $u \equiv a \bmod p$ for an integer a, then there exists $v \in \mathbb{Z}[\zeta]^\times$ such that $u = v^p$.*

While there are several proofs of this result, many make use of class field theory or the p-adic class number formula, which are beyond what is currently available in MATHLIB. For this reason, we have instead opted for a more 'elementary' proof, requiring only some basic results about group cohomology, specifically Hilbert's Theorems 90-94.

Here is an outline of the paper. In Section 2 we fix the informal and formal notation that will be used throughout the paper, explaining the very first issues that appear in the formalization process. In Section 3, we recall how in [Bes+23] we formalized Theorem 3.1, reducing FLT to Theorem 4.1. The main inputs for the proof are described in Figure 1.

The formalization process works backwards from the final goal, gradually reducing the results to known theorems. As we will see, working backwards is key since it ensures all our results will combine to prove our theorem. For this reason we follow a similar structure here, where results are introduced when needed and we gradually reduce our proofs, firstly to Kummer's lemma, then to Hilbert 94, 92,91, and 90 in that order.

Specifically, in Section 4 we reduce the proof of Case 2 to Kummer's lemma, Theorem 5.1. This is mathematically not very difficult, but the proof is rather intricate, and its formalization is quite challenging. We then move on to the heart of our work, the formalization of Kummer's lemma. In Section 5, we prove Kummer's lemma *assuming Hilbert's Theorem 94*, a cohomological result that is historically a precursor of global class field theory. In particular, the only thing that remains to be proven is Theorem 6.1: if L/K is an unramified extension of number fields of odd prime degree, then $[L : K]$ divides the class number of K.

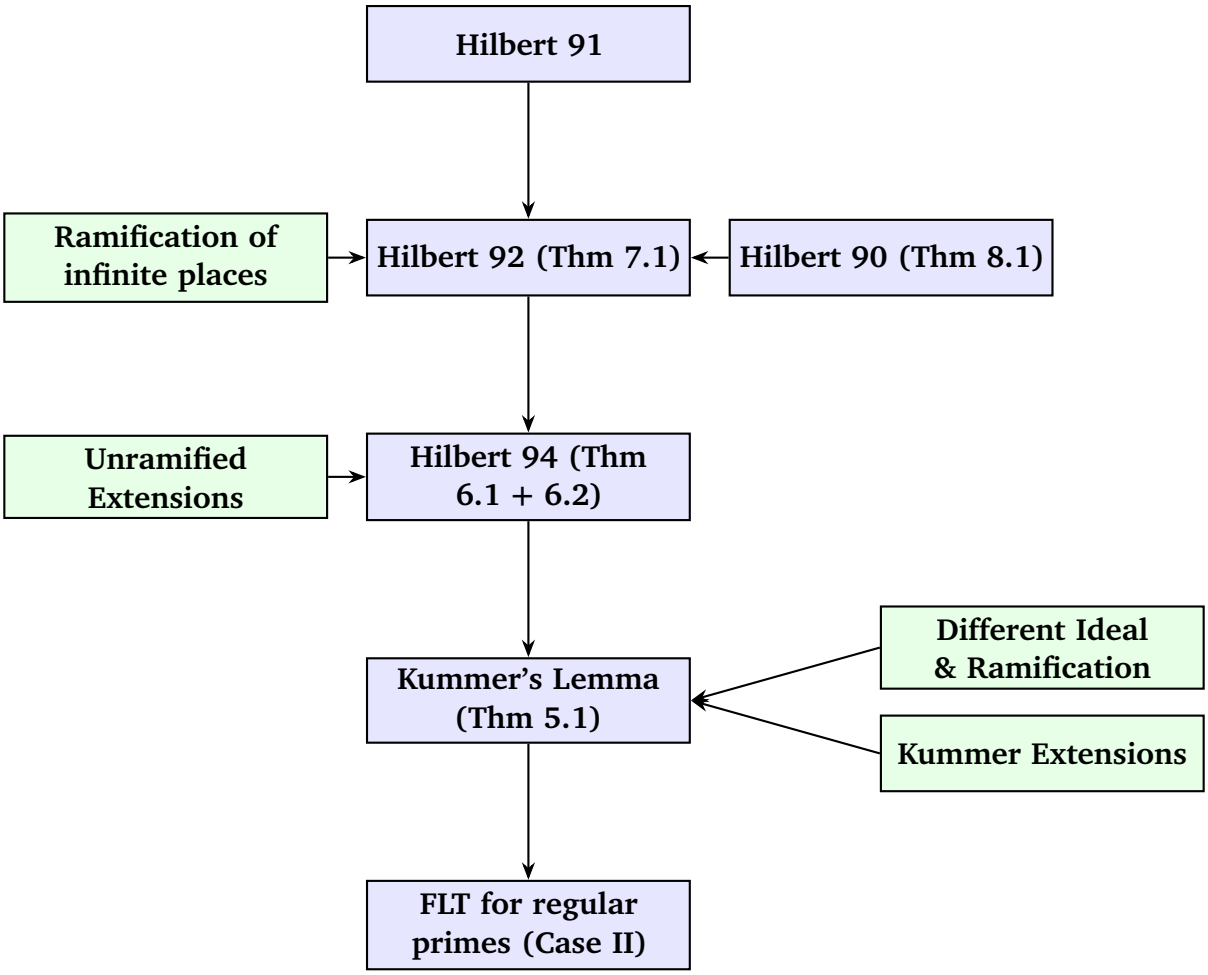

Figure 1: Main inputs into the proof.

Starting with Section 6, our work is basically independent of FLT, and only concerns the cohomology of number fields. We then reduce Theorem 6.1 to Theorem 6.2, and the latter to Hilbert's Theorems 92 and 90, Theorems 7.1 and 8.1. In Section 7 we prove Hilbert's Theorem 92, which is the hardest part of our formalization. The proof we formalize is a simplification of Hilbert's original proof, but it is still subtle and requires a lot of care. In particular it depends on nontrivial results about the units of the ring of integers of number fields. In Section 8 we explain the formalization of the version of Hilbert's Theorem 90 that we need, using what is already in MATHLIB. This finishes the proof of Kummer's lemma, and hence the formalization of FLT for regular primes. In Section 9 we discuss some of the issues we encountered in the formalization process, and how we solved them. Finally, in Section 10 we discuss some future work.

As is clear from the above discussion, the paper works backwards from the final result we want to prove to the results we need. This reflects our formalization process: the final goal, FLT for regular primes, was clear from the beginning and the statement was very easy to formalize. Also the fact that we needed to split the proof into two cases was clear, as all the known approaches follow this strategy. Once Case 1 was done, we moved to Case 2, and again all known approaches use Kummer's lemma. A key observation is that, even if the proof is difficult, the formalization of the statement is easy, so we decided to finish the work assuming Kummer's lemma. Now, as there are several possible ways of proving Theorem 5.1 that involve various complicated objects (cohomology groups, L-functions etc.) it was key to choose an approach that could be formalized in a reasonable time-frame.

Working backwards, we were sure that we were really making progress at any step of the formalization (of course there is always the risk of ending up with something very hard to prove, but in this way we minimize the risk of formalizing unneeded *definitions*). This is a very different strategy with respect to projects like the Liquid Tensor Experiment [CT+22] where the *statement* of the result is already difficult to formalize, not only its proof.

What we learned:

We found that going back to early proofs of theorems and recasting the main ideas with relatively more modern tools, can be highly beneficial for formalization, since these require much less advanced machinery, which in turn simplifies the formalization process. In particular, while Hilbert's theorem 90 is very well-known, theorems 91, 92, and 94 (of [Hil98]) were unknown to the authors before this project, but they are the key to our approach.

The project also uncovered several issues with Lean's MATHLIB, for example, the definition of rings of integers has since changed, due in part to this project highlighting the fact that they would not scale well (as described in Section 9). In particular, it demonstrates the need to test definitions by proving non-trivial theorems.

Acknowledgements

Our project has greatly benefited from the contributions of many members of the MATHLIB community. We are deeply grateful to all those who have been involved in the development of both LEAN and MATHLIB, whose efforts have made our work possible. We would also like to extend our sincere thanks to the anonymous referees for their thorough and thoughtful review of an earlier version of this paper, which led to significant improvements in its clarity and presentation.

2 Informal and formal notation

Throughout the paper, p will be an odd regular prime. Although FLT is a statement about the integers, the proofs all require significant input from algebraic number theory. Here is our basic setup. Let $\mu_p \subset \mathbb{C}$ be the set of p-th roots of unity. We fix $\zeta \in \mu_p$ a primitive root of unity and we will write K for the number field $\mathbb{Q}(\zeta)$. By the definition of regularity, p does not divide the class number of K. The ring of integers of K will be denoted $\mathcal{O}_K$ and note that we have $\mathcal{O}_K = \mathbb{Z}[\zeta]$ (a fact that we formalized in [Bes+23]).

Even if our main result concerns natural numbers and the field $\mathbb{Q}(\zeta)$ only plays an auxiliary role, it appears in most of the results and so we need a formalized definition of $\mathbb{Q}(\zeta)$ that works well in practice. As is customary in formalization projects (see for example [Buz+22, Section 4.3]), it is better to avoid working directly with the field $\mathbb{Q}(\zeta)$ (that would be `Algebra.adjoin ℚ {ζ}`); otherwise all our results would apply only to that extension of $\mathbb{Q}$, and not to any extension that is abstractly isomorphic to it. Instead, we work with any p-th cyclotomic extension of $\mathbb{Q}$, as follows.

```
variable {p : ℕ+} {K : Type*} [Field K] [NumberField K] [IsCyclotomicExtension {p} ℚ K]
```

The class `IsCyclotomicExtension`, that is a fundamental prerequisite for our formalization, has been introduced into MATHLIB during the first steps of our project (see [Bes+23]). The instances `[Field K]` and `[NumberField K]` ensure that K is an extension of $\mathbb{Q}$ that is generated by a primitive p-th root of unity. Note that the assumption that K is a number field is redundant, as it is implied by K being a p-th cyclotomic extension of $\mathbb{Q}$: this result is easily proved in LEAN, but it cannot be an instance (since LEAN has no way of guessing p when it sees a goal of type `NumberField K`) and so `NumberField K` is not found automatically by LEAN and in practice it is more convenient to assume it explicitly. For the same reason, we sometimes use `[CharZero K]` instead of `[NumberField K]` (since some results in MATHLIB use this formulation). Note that in this project p is of type `(p : ℕ+)`, which is the type of positive natural numbers, and in particular it cannot be used where a natural number is expected (for example one cannot write `x ^ p` directly): this is a rather standard annoyance caused by type theory and LEAN has a powerful system to help ignoring these issues (see for example [LM20] for more details). Despite the coercions system, we are sometimes forced to use the coercion `(↑p : ℕ)` explicitly to see p as a natural number. The origin of these problems is that `IsCyclotomicExtension` takes as first argument a set `(S : Set ℕ+)` (this is a design decision made at the beginning of the formalization of the theory of cyclotomic extensions in MATHLIB, and our work highlighted the need for it to be refactored, which has now been completed).

Instead of fixing a primitive p-th root of unity ζ once and for all, it is more convenient in LEAN to work with an unspecified primitive root.

```
variable {ζ : K} (hζ : IsPrimitiveRoot ζ p)
```

One issue that appears is that now `(ζ : K)` has type K, and not $\mathcal{O}_K$ or $\mathcal{O}_K^\times$, forcing us to use several coercions. To make the formalization process as smooth as possible, we usually consider `(hζ.unit' : 𝓞ˣ)`, that is the same as ζ, but seen as a unit of the ring of integers. After having set the relevant `@[simp]` and `@[norm_cast]` tags, we can use various tactics like `push_cast` or `field_simp` to avoid mathematically irrelevant annoyances.

The ring of integers of K is denoted by `𝓞 K`, and MATHLIB contains an extensive library of results about it. For example, the fact that $\mathcal{O}_K$ is a Dedekind domain and the fact that $\mathcal{O}_K = \mathbb{Z}[\zeta]$ are both formalized: the former in the work [Baa+22]. To state that p is a prime, we use `[Fact p.Prime]` (here `(p : ℕ)`): indeed `Nat.Prime` is not a class, but using `Fact` we can record primality as an instance and use typeclass inference. Mathematically, p is regular if the ring of integers of any p-th cyclotomic extension has class number not divisible by p. This is clearly equivalent to the same property for *one fixed model of a p-th cyclotomic extension of* $\mathbb{Q}$ and we decided to formalize the definition this way, using `CyclotomicField p ℚ`. This makes it simpler in practice to show that a given number is regular (the point of having a general K in the project is that most of the theorems concern a cyclotomic extension, so we don't want them to hold only for `CyclotomicField p ℚ`). Here is our definition of being a regular prime.

```
/-- A natural number `n` is regular if `n` is coprime with the cardinal of the class group -/
def IsRegularNumber (n : ℕ) [hn : Fact (0 < n)] : Prop :=
  n.Coprime <| Fintype.card <| ClassGroup (𝓞 <| CyclotomicField ⟨n, hn.1⟩ ℚ)

def IsRegularPrime (p : ℕ) [Fact p.Prime] : Prop := IsRegularNumber p
```

Strictly speaking the definition `IsRegularPrime` is not needed and the main result can be stated using `IsRegularNumber` only: we find nevertheless the use of `IsRegularPrime` closer to informal mathematics. Note that we define the notion of being regular for any positive integer as being coprime with the class number of the corresponding cyclotomic extension, but this is used in practice only for prime numbers: in particular we do not claim that Kummer's lemma holds for regular numbers, it is for example false for $n = 4$. (This is customary in formalized mathematics, since primality is not needed to state the condition, we do not assume it, even if this generality is not mathematically interesting.) Our main is then theorem the following:

```
/-- Fermat's last theorem for regular primes. -/
theorem flt_regular {p : ℕ} [Fact p.Prime] (hreg : IsRegularPrime p) (hodd : p ≠ 2) :
  FermatLastTheoremFor p := by ...
```

Here `FermatLastTheoremFor p` is the statement, existing in MATHLIB,

```
∀ a b c : ℕ, a ≠ 0 → b ≠ 0 → c ≠ 0 → a ^ p + b ^ p ≠ c ^ p
```

Note that technically `FermatLastTheoremFor` is a statement about natural numbers, but the equivalence to the same statement for integers or rationals already exists in MATHLIB.

3 Case 1

The proof of FLT for regular primes is split into two sub-cases. The so called "first case" of FLT is the following (we use $\mathbb{Z}$ in the project rather than $\mathbb{N}$ and we switch to natural numbers at the end to prove `FermatLastTheoremFor`):

Theorem 3.1 (Case 1)**.** *Let $a, b, c \in \mathbb{Z}$ and p a regular prime. If p does not divide abc, then $a^p + b^p \neq c^p$.*

Here is the formalized statement:

```
theorem caseI {a b c : ℤ} {p : ℕ} [Fact p.Prime] (hreg : IsRegularPrime p)
  (caseI : ¬↑p ∣ a * b * c) : a ^ p + b ^ p ≠ c ^ p := ...
```

Note that for $p = 2$ it is easy to see that case 1 cannot hold since the sum of two odd numbers is necessarily even. The formalization of this result was completed on October 13th 2022, a little less than one year later than the starting date of the project. This work is described in [Bes+23], and we will only briefly list the main bits we formalized:

(1) Definitions of cyclotomic fields and cyclotomic extensions.[2]
(2) Explicit formulas for norms, trace (previously defined in [Baa+22]) as well as defining discriminants for number fields.
(3) Computing the discriminant and ring of integers for p-power cyclotomic fields.
(4) Specific results about units in these cyclotomic fields. For example that for $p \neq 2$ a prime, every unit $u \in \mathbb{Z}[\zeta_p]^\times$ can be written as $u = x\zeta_p^n$ for some $n \in \mathbb{Z}$ and $x \in \mathbb{Z}[\zeta_p]^\times$ such that $x \in \mathbb{R}$.

[2] To date these are the only explicit examples of number fields in MATHLIB, although some work in the quadratic case has been done [Baa+23].

(5) The proof of FLT for $n = 3$, which was done independently by one of us (RVdV). Note this case had already been done previously in Isabelle [Oos07].

Our formalization was entirely in LEAN3, and shortly after the end of this task, the transition from LEAN3 to LEAN4 started. Once MATHLIB moved completely to LEAN4, we started updating FLT-REGULAR. For this, we used mathport, a tool developed by the MATHLIB community (especially by Mario Carneiro and Gabriel Ebner) to port LEAN3 projects to LEAN4. Porting FLT-REGULAR, we encountered mainly two issues.

- Coercions (especially from $\mathcal{O}_K^\times$ to $\mathcal{O}_K$ to K) are omnipresent in our project: see [Bes+23, Section 3]. LEAN4 handles coercions in a completely different way from LEAN3, so part of the code had to be rewritten by hand. Although tedious, the same issue had appeared in porting MATHLIB, so the solutions were well understood.
- The way typeclass inference handles multiple inheritance changed in LEAN4: see for example [Wie23]. This caused slowdown in FLT-REGULAR and more generally in MATHLIB[3]. Thanks also to our work (and of course of the MATHLIB community at large), these issues are now solved in MATHLIB. These solutions found in FLT-REGULAR have now been almost completely integrated into mathlib (see Section 9 below for more details).

Another important aspect of our work, described in [Bes+23, Section 4], is integration into MATHLIB. We now have more than 200 pull requests merged that were originally in FLT-REGULAR. Notably, almost all the prerequisites needed to formalize the proof of Case 1 are now in MATHLIB (with the exception of homogenization of polynomials) and we have already started the same process for Case 2. Even if the whole proof of FLT for regular primes is unlikely to be included into MATHLIB (being very technical and specific) we expect that all prerequisites will be upstreamed. Besides improving MATHLIB itself, we saw, especially during the port, that this process reduces the work of maintaining the code. This process can be very tedious due to the continuous development/expansion of MATHLIB, meaning that code is commonly refactored (as better methods/approaches are developed) which leads to projects, not yet included into mathlib, breaking when updated to newer versions of MATHLIB. This is in contrast to other systems with more structured numbered releases.

[3] In the beginning we simply increased the time limit allocations in the project, via the `set_option maxHeartbeats` and `set_option synthInstance.maxHeartbeats` commands, and we worked with the slow code, but this was only a temporary solution.

4 Case 2

Given the formalization of Theorem 3.1 outlined in Section 3, to formalize the proof of FLT for regular primes it is enough to consider the following (which is known as Case 2 of FLT for regular primes):

Theorem 4.1 (Case 2)**.** *Let $p \neq 2$ be a regular prime. Then $x^p + y^p = z^p$ has no solutions such that*

- $xyz \neq 0$.
- $\gcd(x, y, z) = 1$.
- $p \mid xyz$.

Our formalization is the following:

```
/-- CaseII. -/
theorem caseII {a b c : ℤ} {p : ℕ} [hpri : Fact p.Prime]
  (hreg : IsRegularPrime p) (hodd : p ≠ 2)
  (hprod : a * b * c ≠ 0) (hgcd : ({a, b, c} : Finset ℤ).gcd id = 1)
  (caseII : ↑p ∣ a * b * c) : a ^ p + b ^ p ≠ c ^ p := by ...
```

Here is the strategy of the proof that we have formalized (where the main technical step follows [BS66b, Section V.7.1]). Let x, y and z be coprime integers such that $p \mid xyz$ and $x^p + y^p = z^p$. First note that p divides exactly one of x, y, z, and by an easy change of variables we can assume that $p \mid z$. Since we have to show that there is no nontrivial solution with $\gcd(x, y, z) = 1$ and $p \mid z$, it is enough to prove that there is no nontrivial solution such that $p \nmid y$ and $p \mid z$. The statement we are going to prove is then the following:

```
lemma not_exists_Int_solution {p : ℕ} [Fact (p.Prime)] (hreg : IsRegularPrime p)
  (hodd : p ≠ 2) :
 ¬∃ (x y z : ℤ), ¬↑p ∣ y ∧ ↑p ∣ z ∧ z ≠ 0 ∧ x ^ p + y ^ p = z ^ p := by ...
```

In $\mathcal{O}_K$ we have that $p = (1-\zeta)^{p-1}\varepsilon$ for some $\varepsilon \in \mathcal{O}_K^\times$ and the norm of $\zeta - 1$ is p, in particular p divides an integer n in $\mathbb{Z}$ if and only if $\zeta - 1$ divides n in $\mathcal{O}_K$. It follows that it is enough to prove:

```
lemma not_exists_solution' : {p : ℕ+} [Fact (p.Prime)]
 (hreg : (p : ℕ).Coprime <| Fintype.card <| ClassGroup (𝓞 K))
 ¬∃ (x y z : 𝓞 K), ¬(hζ.unit' : 𝓞 K) - 1 ∣ y ∧ (hζ.unit' : 𝓞 K) - 1 ∣ z ∧ z ≠ 0 ∧
  x ^ (p : ℕ) + y ^ (p : ℕ) = z ^ (p : ℕ) := by ...
```

Note that here `(p : ℕ+)` (since we need cyclotomic extensions) and then we are forced to consider the coercion `(p : ℕ)` to take exponentiation. Also, `hreg` is in terms of K rather than `CyclotomicField p ℚ` (mathematically the two notions are of course equivalent): this is because we are proving results about K, so it is more convenient to work with it directly. Since ultimately we will apply our results to the case `K = CyclotomicField p ℚ`, this causes no problems.

Write $z = p^k z_0$ with $z_0 \in \mathbb{Z}$ such that $p \nmid z_0$. It suffices to prove that the more general equation

$$x^p + y^p = \varepsilon(\zeta - 1)^{p(m+1)} z_0^p$$

has no nontrivial solutions with $x, y, z_0 \in \mathcal{O}_K$ such that y and z_0 are not divisible by $1 - \zeta$. Here $m \geq 0$ and $\varepsilon \in \mathcal{O}_K^\times$. The proof follows by a descent argument (which will crucially depend on Kummer's lemma) where one shows that if such a solution exists for some m then one can construct a solution with m replaced by $m - 1$.

We now give more details about the proof, notably explaining where Kummer's lemma is needed. Assume we have $x, y, z \in \mathcal{O}_K$ and $\varepsilon \in \mathcal{O}_K^\times$ such that y and z are not divisible by $1 - \zeta$ and that we have

$$x^p + y^p = \varepsilon(1 - \zeta)^{p(m+1)} z^p \tag{4.1}$$

for some natural number m. In what follows we will keep this choice of ζ fixed and when discussing an arbitrary p-th root of unity we will denote them by η.

Let $\mathfrak{z}$ and $\mathfrak{p}$ denote the ideals generated by z and $\zeta - 1$ respectively. Note that $\mathfrak{p}$ is the only prime ideal of $\mathcal{O}_K$ above p. Then factoring (4.1) as ideals we have

$$\prod_{\eta \in \mu_p} (x + \eta y) = (\zeta - 1)^{p(m+1)} \mathfrak{z}^p.$$

It follows that each $x + \eta y$ is divisible by $(\zeta - 1)$ in $\mathcal{O}_K$. The idea now is to divide each side by $(\zeta - 1)^p$ and then after some manipulations, show that we can create a solution with a smaller power of m on the right hand side. Following [BS66a], one then produces a solution to an equation of the form:

$$u_1 x'^p + y'^p = u_2 (\zeta - 1)^{pm} z'^p. \tag{4.2}$$

Since we already know that $m \geq 1$, we are done *if we can prove that u_1 is a p-th power*. This is the crucial step where we need Kummer's lemma, Theorem 5.1 below. Thanks to it, it is enough to show that u_1 is congruent to some integer modulo p. To prove this, note that since

$(p) = \mathfrak{p}^{p-1}$, there is a unit $u \in \mathcal{O}_K^\times$ such that $pu = (\zeta - 1)^{p-1}$. Substituting in (4.2), we see that $p \mid u_1 x'^p + y'^p$. This implies that there is some $a \in \mathcal{O}_K$ such that u_1 is congruent to a^p modulo p. We then conclude, because for any $x \in \mathcal{O}_K$, we have that x^p is congruent to an integer modulo p.

With the above setup and setting $\pi = \zeta - 1$, the formalization of this argument concludes that we have (see Section 2 for an explanation of the various notations):

```
variable {K : Type*} {p : ℕ+} [hpri : Fact p.Prime] [Field K]
 [NumberField K] [IsCyclotomicExtension {p} ℚ K] (hp : p ≠ 2) [Fintype (ClassGroup (𝓞 K))]
 (hreg : (p : ℕ).Coprime <| Fintype.card <| ClassGroup (𝓞 K)) {ζ : K} (hζ : IsPrimitiveRoot ζ
    p)
 {x y z : 𝓞 K} {ε : (𝓞 K)ˣ} {m : ℕ} (hy : ¬ hζ.unit'.1 - 1 ∣ y) (hz : ¬ hζ.unit'.1 - 1 ∣ z)
 (e : x ^ (p : ℕ) + y ^ (p : ℕ) =   -- i.e. assume we have a solution with m+1
        ε * ((hζ.unit'.1 - 1) ^ (m + 1) * z) ^ (p : ℕ))

lemma exists_solution' : ∃ (x' y' z' : 𝓞 K) (ε₃ : (𝓞 K)ˣ), ¬ π ∣ y' ∧ ¬ π ∣ z' ∧
  x' ^ (p : ℕ) + y' ^ (p : ℕ) = ε₃ * (π ^ m * z') ^ (p : ℕ) --then we get a solution with m
```

5 Kummer's lemma

Kummer's lemma states the following:

Theorem 5.1. *Let p be an odd regular prime and let ζ be a primitive p-th root of unity. If $u \in \mathcal{O}_K^\times$ is a unit such that $u \equiv n \bmod p$ for an integer n, then there exists $v \in \mathcal{O}_K^\times$ such that $u = v^p$.*

Nowadays, one can use more modern tools, such as class field theory to prove Kummer's lemma as follows.

Proof of Theorem 5.1. Let us consider the extension $K(u^{1/p})/K$: it is a Kummer, hence abelian, extension. By a rather elementary argument (see [Was97, second proof of Theorem 5.36] or the proof at the end of this section), the extension is everywhere unramified (here is where the assumption on u is needed), so $K(u^{1/p})$ is contained in L, the Hilbert class field of K. By class field theory, $[L : K]$ is the class number of K and in particular $p \nmid [L : K]$. It follows that the degree of $K(u^{1/p})/K$ cannot be p: the only other possibility is that the degree is 1, so $K(u^{1/p}) = K$ and u has a p-th root in K and hence in $\mathcal{O}_K^\times$. □

The formalization of global class field theory is a long-term project, but we are currently quite far from it, making it impossible to formalize such a proof. There are other proofs, for

example using the p-adic regulator, but again their formalization is unfeasible at the moment. There is also Kummer's original proof [Kum50a] which uses the Bernoulli characterization of regular primes (see 10.1), making the proof more elementary at the cost of proving 10.1, which itself relies on versions of the analytic class number formula for cyclotomic fields [Kum50b].

For these reasons we instead followed a more elementary proof relying on some basic ramification results and Hilbert's Theorems 90, 92 and 94 (see [Hil98] for the original formulation). Those are historically the starting point of modern class field theory, so in a sense our formalized proof is the one above, but written in much more down-to-earth terms.

The formalization of the statement is (notations as in Section 2) the following:

```
theorem eq_pow_prime_of_unit_of_congruent (u : (𝓞 K)ˣ)
  (hcong : ∃ n : ℤ, (p : 𝓞 K) ∣ (u - n : 𝓞 K)) : ∃ v, u = v ^ (p : ℕ) := by ...
```

Note we decided to spell out explicitly the condition that u is congruent to n modulo p, without actually using $\equiv$ in the formal statement. This is of course equivalent, and we felt that the API was better suited to work with division (we could also have worked with ideals, but again this is more cumbersome).

We now describe in more detail the proof we formalized. Let $u \in \mathcal{O}_K^\times$ and $n \in \mathbb{Z}$ such that $u \equiv n \bmod p$. Suppose for a moment that if $w \in \mathcal{O}_K^\times$ is a unit such that $(\zeta - 1)^p \mid w - 1$ then there exists some $v \in K$ such that $v^p = w$. Admitting this claim, we see that with our setup we have $u \equiv a \mod p$ for some integer a. Now this means that $u^{p-1} \equiv 1 \mod p$, which means that $u^{p-1} \equiv 1 \mod (\zeta - 1)^{p-1}$ and hence $u^{p-1} \equiv 1 \mod (\zeta - 1)^p$. Using the claim we then have a v' (which must necessarily be a unit) such that $v'^p = u^{p-1}$. So choosing $v = u/v'$ we see that $v^p = u$ as required.

So it remains to prove the claim, which is formalized as follows:

```
theorem exists_pow_eq_of_zeta_sub_one_pow_dvd_sub_one {u : (𝓞 K)ˣ}
  (hcong : (hζ.unit' - 1 :𝓞 K) ^ (p : ℕ) ∣ (u : 𝓞 K) - 1) : ∃ v : K, v ^ (p : ℕ) = u := by...
```

To see this, assume for contradiction that the claim is false, so u is not a p-th power and let $L = K(u^{1/p})$. The extension L/K is a Kummer extension that by our assumption has degree p. Note that there was no theory of Kummer extensions in MATHLIB when the project began, and we developed it from the ground up. This new material is now fully integrated in the library and it is fairly complete: for example MATHLIB knows that $K(u^{1/p})/K$ is Galois with cyclic Galois group.

We now claim that L/K is unramified. Again we had to develop the theory of unramified extensions from scratch, and this material is now in the process of being integrated into MATHLIB. The formal statement we use to prove unramifiedness is the following:

```
lemma isUnramified (L) [Field L] [Algebra K L]
  [IsSplittingField K L (X ^ (p : ℕ) - C (u : K))] : IsUnramified (𝓞 K) (𝓞 L) := by ...
```

Here L is the splitting field of $X^p - u$ over the cyclotomic field K. Consider the polynomial

$$P_u = \frac{((\zeta - 1)X - 1)^p + u}{(\zeta - 1)^p} \in K[X].$$

First of all we have that $P_u \in \mathcal{O}_K[X]$, it is monic and has degree p. Moreover, in $K[X]$ we have that

$$P_u = \left(X - (\zeta - 1)^{-1}\right)^p + \left(\frac{u}{\zeta - 1}\right)^p.$$

Since we are assuming that u is not a p-th power we have that P_u is irreducible over K. Moreover, the roots of P_u are the

$$\alpha_m := \frac{1 - \zeta^m u^{1/p}}{\zeta - 1},$$

for $m = 0, \dots, p-1$ and so P_u is the minimal polynomial of any of the α_m over K and hence, by Gauss's lemma, over $\mathcal{O}_K$. An explicit computation shows that $X - \alpha_{m_1}$ and $X - \alpha_{m_2}$ are coprime if $m_1 \neq m_2$, and thus P_u is a separable polynomial[4] over $\mathcal{O}_L$ and in particular it is separable over $\mathcal{O}_K/I$ for any maximal ideal $I \subseteq \mathcal{O}_K$. Since clearly $L = K(\alpha_m)$ and α_m has separable polynomial modulo any maximal ideal of $\mathcal{O}_K$, we have that the extension L/K is everywhere unramified. Note that the proof of unramifiedness, although not very complex, is quite intricate, and it required us to develop the theory of unramified extensions. In doing so we formalized, among other things the following (for arbitrary extensions of number fields L/K):

(1) Definition of the relative different ideal $\mathfrak{d}_{L/K} := ((\mathcal{O}_L)^*)^{-1}$ where

$$M^* = \{\alpha \in L |\ \mathrm{Tr}_{L/K}(\alpha M) \in \mathcal{O}_K\}.$$

This is now in MATHLIB.

[4] meaning it is coprime to its derivative.

(2) Proving that if L/K is an extension of number fields and S denotes the set of $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$, then we have

$$\mathfrak{d}_{L/K} = \left(m'_\alpha(\alpha) : \alpha \in S\right)$$

where m_α denotes the minimal polynomial of α.

(3) If $\mathfrak{p}_K, \mathfrak{p}_L$ prime ideals in L, K respectively, with $\mathfrak{p}_L^e \parallel \mathfrak{p}_K$ for $e > 0$, then

$$\mathfrak{p}_L^{e-1} \mid \mathfrak{d}_{L/K}.$$

(4) If $L = K(\alpha)$ and m_α is separable modulo a prime ideal $\mathfrak{p}_K$, then we have that $\mathfrak{p}_K$ is unramified in $\mathcal{O}_L$.

The situation is now the following: we have a unit $u \in \mathcal{O}_K^\times$ that is not a p-th power and moreover the extension $K(u^{1/p})/K$ is everywhere unramified. We need to find a contradiction. Note that we have yet to use regularity of p. It is unlikely that one can finish the proof without some sort of class field theory result that allows one to deduce information about the class group from the existence of an unramified abelian extension. The one we formalize is Hilbert's Theorem 94, whose second part, Theorem 6.1 below, finishes the proof since by regularity p cannot divide the class number of K.

6 Hilbert's Theorem 94

Hilbert's Theorem 94 has two parts to it. Continuing our backwards reasoning, we start with the second one, that we used above to finish the proof of unramifiedness.

Theorem 6.1. *[Hilbert's Theorem 94, part 2] Let L/K be an unramified cyclic finite extension of number fields of odd prime degree, then $[L : K]$ divides the class number of K.*

Proof. To prove the theorem, assume that $[L : K]$ does not divide the class number and note that if I is any ideal of $\mathcal{O}_K$ such that I_L, the extension to $\mathcal{O}_L$ of I, is principal then I is automatically principal. Indeed, we have $\mathrm{Norm}_{L/K}(I_L) = I^{[L:K]}$ and, I_L being principal means that $I^{[L:K]}$ is principal. Since $[L : K]$ is coprime to the class number we have that I is principal. In particular, we see that it is enough to show that there is a non-principal ideal of $\mathcal{O}_K$ that becomes principal in $\mathcal{O}_L$. This is precisely the content of part 1 of Hilbert's Theorem 94, Theorem 6.2 below. □

A formalization of the above argument is the following. We include also the proof, that is very short and follows our informal proof above. Theorem 6.2 below is the declaration `exists_not_isPrincipal_and_isPrincipal_map` is.

```
theorem dvd_card_classGroup_of_isUnramified_isCyclic {K L : Type*}
  [Field K] [Field L] [NumberField K] [NumberField L] [Algebra K L]
  [FiniteDimensional K L] [IsGalois K L] [IsUnramified (𝓞 K) (𝓞 L)] [IsCyclic (L ≃ₐ[K] L)]
  (hKL : Nat.Prime (finrank K L))
  (hKL' : finrank K L ≠ 2) :
  finrank K L ∣ Fintype.card (ClassGroup (𝓞 K)) := by
 obtain ⟨I, hI, hI'⟩ := exists_not_isPrincipal_and_isPrincipal_map K L hKL hKL'
 have := Fact.mk hKL
 rw [hKL.dvd_iff_not_coprime]
 exact fun h ↦ hI (isPrincipal_of_isPrincipal_pow_of_coprime h
  (Ideal.isPrincipal_pow_finrank_of_isPrincipal_map hI'))
```

Note that `IsCyclic (L ≃ₐ[K] L)` is automatic by the other assumptions, but we find it more convenient to explicitly add it. In the applications, it is found by typeclass inference, so this does not cause any issue.

We now move on to the first part of Hilbert's Theorem 94, which states that:

Theorem 6.2. *[Hilbert's Theorem 94, part 1] Let L/K be an unramified cyclic extension of number fields of odd prime degree, then there is a non-principal ideal of $\mathcal{O}_K$ that becomes principal in $\mathcal{O}_L$.*

Proof. This is a consequence of Hilbert's Theorem 92, Theorem 7.1 below. Let $\eta \in \mathcal{O}_K^\times$ be a unit with $\mathrm{Norm}_{L/K}(\eta) = 1$ and such that for all $w \in \mathcal{O}_K^\times$ we have $\eta \neq w/\sigma(w)$, where σ is a fixed generator of $\mathrm{Gal}(L/K)$. By Hilbert's Theorem 90, Theorem 8.1 below, there is $\beta \in \mathcal{O}_K$ such that $\beta \neq 0$ and $\beta = \sigma(\beta)\eta$. We let $I := \mathcal{O}_K \cap (\beta)$, the ideal of $\mathcal{O}_K$ given by the ideal of $\mathcal{O}_L$ generated by β. We claim that I satisfies the required properties. Suppose for a moment that $I\mathcal{O}_L = (\beta)$. This obviously implies that the extension of I to $\mathcal{O}_L$ is principal. If I were principal generated by γ, there would be a unit $w \in \mathcal{O}_K^\times$ such that $\beta = \gamma w$. Substituting into $\beta = \sigma(\beta)\eta$, since $\sigma(w) = w$ by $w \in \mathcal{O}_K$, we get $\eta = \gamma/\sigma(\gamma)$ that is absurd. In particular I is not principal.

We now prove that $I\mathcal{O}_L = (\beta)$. Since $\sigma^{-1}(\beta) = \sigma^{-1}(\eta)\beta$, we have that $\sigma^{-1}(I)\mathcal{O}_L = (\beta)$. Since L/K is unramified, this implies that $I\mathcal{O}_L = (\beta)$ (this is a technical point where we use the unramifiedness assumption to factor $I\mathcal{O}_L$ into product of prime ideals). □

Our formalization of the above theorem is the following:

```
theorem exists_not_isPrincipal_and_isPrincipal_map (K L : Type*)
  [Field K] [Field L] [NumberField K] [NumberField L] [Algebra K L]
  [FiniteDimensional K L] [IsGalois K L] [IsUnramified (𝓞 K) (𝓞 L)] [h : IsCyclic (L ≃ₐ[K] L
    )]
  (hKL : Nat.Prime (finrank K L)) (hKL' : finrank K L ≠ 2) :
  ∃ I : Ideal (𝓞 K), ¬I.IsPrincipal ∧ (I.map (algebraMap (𝓞 K) (𝓞 L))).IsPrincipal := by ...
```

The formal proof is a faithful translation of the informal one above.

7 Hilbert's Theorem 92

The main technical input in our formalization of Kummer's lemma is the following result:

Theorem 7.1 (Hilbert's Theorem 92)**.** *Let K/k be a cyclic extension of number fields of odd prime degree and let σ be a generator of the Galois group. Then there exists a unit $u \in \mathcal{O}_K^\times$ such that $\mathrm{Norm}_{K/k}(u) = 1$ and for all $\varepsilon \in \mathcal{O}_K^\times$ we have $u \neq \varepsilon/\sigma(\varepsilon)$.*

We formalize the above statement as `Hilbert92`:

```
lemma Hilbert92
  [Algebra k K] [IsGalois k K] [FiniteDimensional k K](hKL : Nat.Prime (finrank k K))
  (hpodd : finrank k K ≠ 2) (σ : K ≃ₐ[k] K) (hσ : ∀ x, x ∈ Subgroup.zpowers σ) :
  ∃ u : (𝓞 K)ˣ, Algebra.norm k (u : K) = 1 ∧ ∀ ε : (𝓞 K)ˣ, (u : K) ≠ ε / (σ ε : K) :=
```

Note that by Hilbert's Theorem 90, Theorem 8.1 below, we know that any such u must be of the form $w/\sigma(w)$ for $w \in \mathcal{O}_K$. So the content is in showing that w cannot always be chosen to be a unit. This translates to saying that a certain cohomology group does not vanish as opposed to the usual vanishing result associated with Hilbert's Theorem 90. As remarked in [SD01, Page 76], the cohomological point of view does not make the proof of this theorem easier, so we instead follow the classical proof described therein, which also has the advantage of being more amenable to formalization given the current state of MATHLIB, but does rely on Hilbert 90, which we do prove by cohomological means.

The construction of a unit satisfying the requirements of Hilbert's Theorem 92 will be a consequence of the existence of a particular set of units.

7.1 Fundamental system of units

***Definition* 7.2.** *Let σ be a generator of $\mathrm{Gal}(K/k)$ (with K/k as in Theorem 7.1) and let r be $\mathrm{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times)$. Let $\mathcal{U}'_{K/k} = \mathcal{O}_K^\times/\mathcal{O}_k^\times$ and let $\mathcal{U}'_{K/k,\mathrm{tors}}$ denote the torsion subgroup. Let*

$$\mathcal{U}_{K/k} = \mathcal{U}'_{K/k}/\mathcal{U}'_{K/k,\mathrm{tors}},$$

which we note is naturally a $\mathbb{Z}[\mathrm{Gal}(K/k)]$*-module. Then a fundamental system of* $r+1$ *units is a choice of* $r+1$ *elements* $\{h_i\}$ *of* $\mathcal{U}_{K/k}$ *such that*

$$\mathcal{U}_{K/k}/\langle h_i\rangle_{\mathbb{Z}[\mathrm{Gal}(K/k)]}$$

is finite with minimal index.

Remark 7.3. Note that this definition of fundamental system of units differs from perhaps the more traditional one, where the final quotient is by the $\mathbb{Z}$-module generated by the h_i (as opposed to the $\mathbb{Z}[\mathrm{Gal}(K/k)]$-module we use).

We are going to show that a fundamental system of units exists. Instead of working directly with $\mathcal{U}_{K/k}$, we find it more convenient to formalize a more general situation and then restrict to the specific setting above. We begin with any additive commutative group G playing the role of $\mathcal{U}_{K/k}$, which we also assume is a A-module, where $A = \mathbb{Z}[\mathrm{Gal}(K/k)]$. Note that the natural notation for $\mathcal{U}_{K/k}$ is multiplicative rather than additive, but to use the language of modules we are forced to work with additive groups.

Remark 7.4. For convenience in the LEAN code, we take $A = \mathbb{Z}[\zeta]$ identified to $\mathbb{Z}[\mathrm{Gal}(K/k)]$ via $\zeta \mapsto \sigma$ (recall that σ is a fixed generator of the Galois group).

We start by defining the notion of *system of s units* where s is a natural number. It is just a set of s elements of G that are linearly independent over A.

```
structure systemOfUnits (G : Type*) [AddCommGroup G] (s : ℕ) where
 units : Fin s → G  --A choice of s elements of G
 linearIndependent : LinearIndependent A units
```

We prove that if G is free as $\mathbb{Z}$-module of rank $s(p-1)$, then a system of s units always exists.

We now move on to the definition of *fundamental systems of r units*. We start by introducing the notion of *maximal system* of s units.

```
abbrev systemOfUnits.IsMaximal {s : ℕ} {p : ℕ+} {G : Type*} [AddCommGroup G]
  [Module A G] (sys : systemOfUnits (G := G) p s) :=
  Fintype (G ⧸ Submodule.span A (Set.range sys.units))
```

By definition, being maximal means that the quotient by the submodule generated by the elements of the system of units is finite. We then prove that if there is a system of s units then there is a maximal one if $\mathrm{rk}_{\mathbb{Z}}(G) = s(p-1)$.

A system of s units is *fundamental* if it is maximal and the submodule generated by the elements of the system has index smaller than those generated by any other maximal system.

```
def systemOfUnits.IsFundamental [Module A G] (h : systemOfUnits p G s) :=
 ∃ _ : h.IsMaximal, ∀ (S : systemOfUnits p G s) (_ : S.IsMaximal), h.index ≤ S.index
```

We then prove that a fundamental system of s units always exists if G is free as $\mathbb{Z}$-module of rank $s(p-1)$. The key property of fundamental systems of units is the following.

Lemma 7.5. *Let $a_0, \dots, a_{s-1}$ be integers not all divisible by p and $\{h_i\}$ a fundamental system of s units, then*

$$\prod_{i=0}^{s-1} h_i^{a_i} \neq u/\sigma(u)$$

for any $u \in \mathcal{U}_{K/k}$.

Our formalization is (note the additive notation) the following:

```
lemma corollary [Module A G] (S : systemOfUnits p G s) (hs : S.IsFundamental)
  (a : Fin s → ℤ) (ha : ∃ i , ¬ (p : ℤ) ∣ a i) :
  ∀ g : G, (1 - zeta p) • g ≠ Σ i, a i • S.units i := by ...
```

Here `zeta : CyclotomicIntegers p := AdjoinRoot.root _` is the fixed root of the p-th cyclotomic polynomial in A, that corresponds to the primitive p-th root of unity ζ (and that acts as the fixed generator σ).

7.2 Hilbert 91

We now go back to our specific situation of a cyclic field extension K/k. We want to show that a system of fundamental $r+1$ units exists in the case $r = \mathrm{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times)$ and $G = \mathcal{U}_{K/k}$. As $\mathcal{U}_{K/k}$ is torsion-free and hence free (as a $\mathbb{Z}$-module), this amounts to showing its rank is $(r+1)(p-1)$. This is essentially the content of Hilbert's Theorem 91. We begin by defining the group $\mathcal{U}'_{K/k} = \mathcal{O}_K^\times/\mathcal{O}_k^\times$ as follows:

```
def RelativeUnits (k K : Type*) [Field k] [Field K] [Algebra k K] :=
 ((𝓞 K)ˣ ⧸ (MonoidHom.range <|
        Units.map (algebraMap (𝓞 k) (𝓞 K) : (𝓞 k) →* (𝓞 K))))
```

Here `MonoidHom.range <| Units.map (algebraMap (𝓞 k) (𝓞 K) : (𝓞 k) →* (𝓞 K))` denotes the image of the units in k under the natural embedding into $\mathcal{O}_K^\times$. Since we are going to work with a fixed generator of the Galois group, we find it more convenient to package together all the data we have as `relativeUnitsWithGenerator`.

```
def relativeUnitsWithGenerator (_hp : Nat.Prime p) (_hKL : finrank k K = p)
(σ : K ≃ₐ[k] K) (_hσ : ∀ x, x ∈ Subgroup.zpowers σ) :=
 RelativeUnits k K
```

This is the same as `RelativeUnits`, but it contains the choice of a generator σ. Finally, we define our additive torsion-free group $\mathcal{U}_{K/k} = \mathcal{U}'_{K/k}/\mathcal{U}'_{K/k,\mathrm{tors}}$ as follows:

```
local notation "G" =>
 Additive (relativeUnitsWithGenerator p hp hKL σ hσ) /
  AddCommGroup.torsion (Additive (relativeUnitsWithGenerator p hp hKL σ hσ))
```

Here, if `H` is a multiplicative group, `Additive H` is the same group, but with additive notation. As explained above we are forced to use it, and it causes a little bit of friction, but all the relevant results to go from `H` to `Additive H` were already in MATHLIB. We show that if we consider G as a $\mathbb{Z}[X]$-module via $X \mapsto \sigma$, then it is torsion with respect to the subgroup generated by the cyclotomic polynomial. This endows G with a structure of an A-module. Moreover, we show that it has rank (as a $\mathbb{Z}$-module) equal to $(r+1)(p-1)$ (this step is rather delicate: we need first of all to take care of the quotient by the torsion submodule and then we use that our extension is unramified at infinite places since p is assumed to be odd).

Putting it all together, we can use our general existence result above to show that there is in fact a fundamental system of $r+1$ units for G as claimed by Hilbert's Theorem 91:

```
lemma Hilbert91 :
 ∃ S : systemOfUnits p G (NumberField.Units.rank k + 1), S.IsFundamental :=
 systemOfUnits.IsFundamental.existence p hp G
 (NumberField.Units.rank k + 1) (finrank_G p hp hKL σ hσ)
```

7.3 Proving Hilbert's Theorem 92

We can now finish the proof of Hilbert's Theorem 92, reducing the proof of Fermat's Last Theorem for regular primes to Hilbert's Theorem 90.

Let K/k be as in 7.1. Remember that in particular p is an odd prime and that σ is a generator of $\mathrm{Gal}(K/k)$. Recall that $r = \mathrm{rk}_{\mathbb{Z}}(\mathcal{O}_k^\times)$ and let h_i be a fundamental system of $r+1$ units for $\mathcal{U}_{K/k}$, that exists by Hilbert's Theorem 91 above. We denote by H_i fixed lifts to elements of $\mathcal{O}_K^\times$. We fix $h \in \mathbb{N}$ such that k contains a p^h-th root of unity ν but no p^{h+1}-th root (note we allow h to be zero). Let $\xi = \nu^{p^{h-1}}$ which is now a p-th root of unity as above, with the convention that if $h = 0$ we have $\xi = \nu = 1$.[5]

[5] In the formalization this convention is automatic, as $0 - 1 = 0$ for natural numbers in LEAN.

With these notations the proof proceeds as follows (in the formalization most of the statements are actually more general than those below, for example stated for any family of r elements of $\mathcal{O}_K^\times$ when the fact that being a fundamental system of r units is not needed):

(1) By Hilbert's Theorem 90, Theorem 8.1 below, we know that, since ξ has norm 1, we can write $\xi = \varepsilon/\sigma(\varepsilon)$ for some $\varepsilon \in \mathcal{O}_K$.

(2) We can assume that there is some $E \in \mathcal{O}_K^\times$ such that

$$\xi = E/\sigma(E)$$

as otherwise we could take ξ as the element required by 7.1.

(3) Note that from $\xi = E/\sigma(E)$ we have that $\mathrm{Norm}_{K/k}(E) = E^p$.

(4) Let $\eta_i = \mathrm{Norm}_{K/k}(H_i)$ for $i \in \{0, \dots, r\}$ and let $\eta_{r+1} := \mathrm{Norm}_{K/k}(E) = E^p$ (again most of the formal statements are for general η_i).

(5) There exist $a, a_i \in \mathbb{Z}$ for $i \in \{0, \dots, r+1\}$ such that

$$\prod_{i=0}^{r+1} \eta_i^{a_i} = \nu^{ap}$$

with a_{i_0} not divisible by p for some i_0. Moreover, if $\nu = 1$ (i.e. $h = 0$) then we can take i_0 to be different from $r+1$.

(6) With these exponents a_i in hand we can now construct our element. Set

$$J := \nu^{-a} \prod_{i=0}^{r+1} H_i^{a_i}$$

where we set $H_{r+1} = E$. We need to show it satisfies the required properties.

(7) Taking its norm we have that

$$\mathrm{Norm}_{K/k}(J) = \left(\prod_{i=0}^{r+1} \eta_i^{a_i} \right) \nu^{-ap}$$

which is 1 by the condition on the a_i's in (5).

(8) Now if J was of the form $\varepsilon/\sigma(\varepsilon)$ for some unit ε, then the same would be true of its image in $\mathcal{U}_{K/k}$. Its image is

$$\nu^{-a} \prod_{i=0}^{r} h_i^{a_i} \cdot E^{a_{r+1}}.$$

Now, since $\nu \in \mathcal{O}_k^\times$, its image in the quotient is 1 (remember that here we are using multiplicative notation). Moreover, since $E^p = \mathrm{Norm}_{K/k}(E)$ also belongs to $\mathcal{O}_k^\times$ we have that its image is 1, so the image of E is torsion. Being $\mathcal{U}_{K/k}$ torsion-free, we have that E becomes equal to 1 in the quotient and the image of J is

$$\prod_{i=0}^{r} h_i^{a_i}.$$

(9) By Lemma 7.5 to conclude the proof it is enough to show that not all of the a_i for $i \in \{0, \dots, r\}$ are divisible by p. Assume for contradiction this is the case, then a_{r+1} must be divisible by p. Now, this means $h \neq 0$ since otherwise this would contradict our choice of a_i's. But now this means that $\eta_{r+1} = \mathrm{Norm}_{K/k}(E) = E^p$ is the p-th power of a unit in k (this follows from (5)). In particular E is a *unit* now in k. But this means that $\sigma(E) = E$, in particular $\xi = 1$, but this cannot be the case as we have already shown $h \neq 0$.

The proof of the last two points are inlined in the proof of `almostHilbert92`, that is Hilbert's Theorem 92 with the additional assumption that K/k is unramified at all infinite places.

Remark 7.6. Note that we have slightly simplified the proof of Hilbert's Theorem 92 as found in [Hil98], which splits into two cases, the first when K does not contain a p-th root and the second where it contains a p^h-th root (but not a p^{h+1}-th root) for some h. Our proof instead allows $h = 0$ and so follows the second case.

8 Hilbert's Theorem 90

Hilbert's Theorem 90 is a now a classical result in Galois cohomology, and MATHLIB already contains a version of (a generalization of) it, thanks to the work of Amelia Livingston, see [Liv23]. We explain in this section the precise statement we need, and how to get there given what is already in MATHLIB.

The statement we needed above is the following, matching Hilbert's original formulation.

Theorem 8.1 (Hilbert's Theorem 90, concrete version)**.** *Let L/K be a cyclic extension of fields and let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. If $\eta \in L$ is such that $\mathrm{Norm}_{L/K}(\eta) = 1$, then there exists an $\varepsilon \in \mathcal{O}_L$ such that $\varepsilon \neq 0$ and $\eta\sigma(\varepsilon) = \varepsilon$.*

Proof. By clearing denominators, it is enough to prove that there is $\varepsilon \in L$ such that $\varepsilon \neq 0$ and $\eta = \varepsilon/\sigma(\varepsilon)$. We then deduce the theorem from Noether's generalization of Hilbert's Theorem

90, Theorem 8.2 below. Let $c\colon \mathrm{Gal}(L/K) \to L^\times$ be the function $\tau \mapsto \prod_{i=0}^{n} \sigma^i(\eta)$, where $n \in \mathbb{N}$ is the unique natural number smaller than the order of $\mathrm{Gal}(L/K)$ such that $\sigma^n = \tau$. Using that $\mathrm{Norm}_{L/K}(\eta) = \prod_{\tau \in \mathrm{Gal}(L/K)} \tau(\eta) = 1$ we have that c is a cocycle, i.e. $c(\tau_1\tau_2) = \tau_1(c(\tau_2))c(\tau_1)$. Since $H^1(G, L^\times)$ is trivial by Theorem 8.2, we have that c is a coboundary. By definition this means that there is $x \in L$ such that $c(\tau) = \tau(x)/x$ for all $\tau \in \mathrm{Gal}(L/K)$ and in particular $c(\sigma) = \sigma(x)/x$. Since $c(\sigma) = \eta$, we have that $x\eta = \sigma(x)$ and $\varepsilon = x^{-1}$ satisfies the conditions of the theorem. □

Here is our formalization:

```
variable {K L : Type*} [Field K] [Field L] [Algebra K L]
 [IsGalois K L] [FiniteDimensional K L]
 {A B : Type*} [CommRing A] [CommRing B] [Algebra A B] [Algebra A L] [Algebra A K]
 [Algebra B L] [IsScalarTower A B L] [IsScalarTower A K L] [IsFractionRing A K]
 [IsDomain A] [IsIntegralClosure B A L] [IsDomain B]

lemma Hilbert90_integral (σ : L ≃ₐ[K] L) (hσ : ∀ x, x ∈ Subgroup.zpowers σ)
  (η : B) (hη : Algebra.norm K (algebraMap B L η) = 1) :
  ∃ ε : B, ε ≠ 0 ∧ η * galRestrict A K L B σ ε = ε := by ...
```

Note that in the formalization, instead of working with $\mathcal{O}_K$ and $\mathcal{O}_L$ (the integral closure of $\mathbb{Z}$ in K and L respectively), we decided to work with general integral domains A and B such that B is in the integral closure of A in L; see Section 9 for more details about this design decision.

The formal proof follows the informal one, clearing denominators (a step that in Lean is not completely trivial since we need to consider the restriction of σ to B) and deducing the theorem from Hilbert's theorem 90:

```
lemma Hilbert90 {η : L} (hη : Algebra.norm K η = 1) :
  ∃ ε : L, η = ε / σ ε := by ...
```

Note that even if technically the statement does not contain the fact that $\varepsilon \neq 0$, this is automatic: if $\varepsilon = 0$, then $\sigma(\varepsilon) = 0$ and hence $\varepsilon/\sigma(\varepsilon) = 0$ (remember that in Lean division by 0 returns 0), so $\eta = 0$, which is impossible because $\mathrm{Norm}_{L/K}(\eta) = 1$.

Everything is now reduced to the following.

Theorem 8.2 (Noether's generalization of Hilbert's Theorem 90)**.** *Let L/K be a finite Galois extension of fields with Galois group G. Then $H^1(G, L^\times)$ is trivial.*

This is a nowadays classical result in group cohomology, and we will not recall the proof. Thanks to the formalization project [Liv23] by Amelia Livingston, it is already present in MATHLIB.

```
/-- Noether's generalization of Hilbert's Theorem 90: given a finite extension of fields and a
    function `f : Aut_K(L) → L^×` satisfying `f(gh) = g(f(h)) * f(g)` for all `g, h : Aut_K(L)`, there
    exists `β : L^×` such that `g(β)/β = f(g)` for all `g : Aut_K(L).` -/
theorem isMulOneCoboundary_of_isMulOneCocycle_of_aut_to_units
  (f : (L ≃ₐ[K] L) → Lˣ) (hf : IsMulOneCocycle f) :
  IsMulOneCoboundary f := by ...
```

Here `IsMulOneCocycle` and `IsMulOneCoboundary` are defined as follows (where M is any G module, for a group G):

```
def IsMulOneCocycle (f : G → M) : Prop := ∀ g h : G, f (g * h) = g • f h * f g
```

```
def IsMulOneCoboundary (f : G → M) : Prop := ∃ x : M, ∀ g : G, g • x / x = f g
```

Note that group cohomology here is defined in very concrete terms, as cocycles modulo coboundaries, and not via abstract machinery like derived functors (that exist in MATHLIB). Even if at some point MATHLIB will need the connection between these two definitions, the current design choice is very convenient for us, since it allowed us to prove the explicit theorem we need quickly.

9 Implementation issues

We now describe two implementation issues we encountered during our formalization project. As the problem of the coercions from $\mathcal{O}_K^\times$ to $\mathcal{O}_K$ to K and the diamonds related to characteristic zero fields are already discussed in [Bes+23, Section 3], we will not discuss those.

After the port to LEAN4, we noticed that the project was very slow in several places, making it almost impossible to progress with the formalization. In collaboration with the MATHLIB community (especially Matthew Ballard, Kevin Buzzard and Floris van Doorn), we identified that the main bottleneck was the definition of the ring of integers of a number field in MATHLIB, that was:

```
def RingOfIntegers := integralClosure ℤ K
@[inherit_doc] scoped notation "𝓞" => NumberField.ringOfIntegers
```

In general, if A is an R-algebra, the type of `integralClosure R A` is `Subalgebra R A`. This has the advantage that a lot of instances, for example `CommRing (𝓞 K)`, are found automatically by LEAN. On the other hand, it causes the following drawback. MATHLIB contains the following instance, where α is a type endowed with `SMul A α`, that is a scalar multiplication by A.

```
instance [SMul A α] (S : Subalgebra R A) : SMul S α := ...
```

Mathematically this simply means that if we know how to multiply elements of α by any `(a : A)` we can also multiply elements of α by any `(s : S)`. In particular, any time an instance like `SMul (𝓞 K) (𝓞 K)` is needed (for example looking for `Module (𝓞 K) (𝓞 K)`), LEAN will look for an instance of `SMul K (𝓞 K)` (a mathematically meaningless problem), and this search will of course fail. What we realized is that this search is rather slow to fail, and, due to the intricacies of the algebra hierarchy in MATHLIB, it is performed many times. We tried to manually lower the priority of the above instance, but this did not solve the problem. Indeed it is sometimes difficult to control the path chosen by the typeclass inference system, and this solution would not scale anyway. In the pull request #12386 we then decided to change the definition of `ringOfIntegers` to the following

```
def RingOfIntegers : Type _ := integralClosure ℤ K
```

The only difference with the above one is that the type of `𝓞 K` is now `Type _` rather than `Subalgebra ℤ K`. To be precise, `𝓞 K` is now the underlying type of `integralClosure ℤ K`: this means that, for example, the following instance

```
instance : CommRing (𝓞 K) := inferInstanceAs (CommRing (integralClosure _ _))
```

has to be added by hand (here the command `inferInstanceAs` allows LEAN to see through the definition of `RingOfIntegers`). On the other hand, it also means that the instance from `SMul K (𝓞 K)` to `SMul (𝓞 K) (𝓞 K)` is not even considered when solving `Module (𝓞 K) (𝓞 K)`. This simple modification made essentially all MATHLIB's files related to ring of integers of number fields much faster (see the benchmark results) and drastically improved the speed of FLT-REGULAR. Note that the number of instances that have to be added by hand is quite limited, and the gain in speed is huge: we expect that a similar modification will be needed in MATHLIB in the future for other analogous situations, for example in the definition of the adele ring of a global field.

Another issue is related to field extensions: if L/K is such an extension, then $\mathcal{O}_L$ is naturally an $\mathcal{O}_K$-algebra. If moreover K and L are number fields, it is easy to prove that mathematically $\mathcal{O}_L$ "is" the integral closure of $\mathcal{O}_K$ in L. However, it is not possible in LEAN to prove the naive equality of types `𝓞 L = integralClosure (𝓞 K) L`, since the correct formal translation of this

result is a datum of an isomorphism (as $\mathcal{O}_K$-algebras) between $\mathcal{O}_L$ and the integral closure of $\mathcal{O}_K$ in L. Working with such an isomorphism can be annoying, as it will appear several times. To avoid this issue, we decided to work more generally in the so-called *AKLB setting*:

```
variable {A K L B : Type*} [CommRing A] [CommRing B] [Field K] [Field L]
  [Algebra A B] [Algebra A L] [Algebra A K] [Algebra B L]
  [IsScalarTower A B L] [IsScalarTower A K L] [IsFractionRing A K] [IsIntegralClosure B A
    L]
```

Any result holding in this setting will apply both to `B = 𝒪 L` and to `B = integralClosure (𝒪 K) L`, allowing very often to avoid the use of the isomorphism above (one may assume `IsIntegralClosure ℤ A K` to state that A "is" $\mathcal{O}_K$). This setting is very common in algebraic number theory, and we believe this way of formalizing it should be used in MATHLIB every time it is possible.

10 Future work

As explained in [Bes+23, Section 4], one peculiar aspect of our project is that the integration into MATHLIB is happening in real time (for example this was not happening at all for the LTE). Even if we don't think the full proof of Fermat's Last Theorem for regular primes should be included into MATHLIB (as it is very technical and mathematically superseded by more modern approaches), most of the prerequisites we formalized are fundamental results in algebraic number theory and should move to the main library. We estimate that of the approximately $10k$ lines of the project, around $6k$ lines should end up in mathlib of which roughly $3k$ are already present. The process of opening pull requests from FLT-REGULAR to MATHLIB never stopped, and we expect that all the relevant material will end up in MATHLIB at some point. One notable example of this process is the proof of Fermat's Last Theorem for $n = 3$, that is now in MATHLIB. This rather nontrivial case, along with $n = 4$ (also in MATHLIB), will be required for Kevin Buzzard's project of formalizing a proof of the full Fermat's Last Theorem, as modern proofs only cover prime exponents $p \geq 5$.

Concerning future formalizations, one natural question that is left by the current status of FLT-REGULAR is that the condition for a prime of being regular is rather abstract, and difficult to prove in practice. Indeed, the computation of the class number of $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ is a difficult problem, even on paper. Thanks to Xavier Roblot's work, [Rob], Minkowski's bound is in MATHLIB. In particular it is easy to prove that both $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ and $\mathbb{Z}[e^{\frac{2\pi i}{5}}]$ are principal ideal domains (since the Minkowski bound is 1 in these cases), and hence 3 and 5 are regular

primes (we also know that 2 is regular) and the case $n = 5$ of Fermat's Last Theorem follows. This is to our knowledge the first formalization of the nonexistence of nontrivial solutions to

$$x^5 + y^5 = z^5.$$

A natural question is to give more explicit examples of regular primes. One can prove that $\mathbb{Z}[e^{\frac{2\pi i}{p}}]$ is principal for all $p \leq 19$ (the converse also holds), but the proof is more and more involved: indeed Minkowski's bound becomes exponentially larger and one has to check a lot of cases by hand, but more recently we have completed the cases 7, 11 and 13. Note that this is very cumbersome and it cannot work for $p > 19$ (for example $\mathbb{Z}[e^{\frac{2\pi i}{23}}]$ has class number 3, so 23 is regular). A better approach is to prove regularity via the following result of Kummer [Kum50b] (see also [Was97, Theorem 5.34]):

Theorem 10.1. *An odd prime p is regular if and only if p does not divide the denominator of the Bernoulli number B_n for $n = 2, 4, \ldots, p-3$.*

Since Bernoulli numbers are very easy to compute (and already in MATHLIB) this criterion gives a very easy way of checking whether a given p is regular (for example one immediately obtains that the only irregular primes $p \leq 100$ are 37, 59 and 67). One possible proof of Theorem 10.1 uses the p-adic class number formula, which is proved using p-adic L-functions. The basic theory of p-adic L-functions has been formalized by Narayanan in LEAN3 (see [Nar23]), and a port to LEAN4 is work in progress. For these reasons we believe that the formalization of Theorem 10.1 is within reach, and we plan to accomplish it in the near future.

References

[Baa+23] A. Baanen, A. J. Best, N. Coppola, and S. R. Dahmen. "Formalized Class Group Computations and Integral Points on Mordell Elliptic Curves". In: *Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs*. CPP 2023. Boston, MA, USA: Association for Computing Machinery, 2023, 47–62. ISBN: 9798400700262. DOI: 10.1145/3573105.3575682. URL: https://doi.org/10.1145/3573105.3575682.

[Baa+22] A. Baanen, S. R. Dahmen, A. Narayanan, and F. A. E. Nuccio Mortarino Majno di Capriglio. "A Formalization of Dedekind Domains and Class Groups of Global Fields". In: *J. Autom. Reason.* 66.4 (2022), pages 611–637. DOI: 10.1007/s10817-022-09644-0. URL: https://doi.org/10.1007/s10817-022-09644-0.

[Bes+23] A. J. Best, C. Birkbeck, R. Brasca, and E. Rodriguez Boidi. “Fermat’s Last Theorem for Regular Primes”. In: *14th International Conference on Interactive Theorem Proving (ITP 2023)*. Edited by A. Naumowicz and R. Thiemann. Volume 268. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023, 36:1–36:8. ISBN: 978-3-95977-284-6. DOI: 10.4230/LIPIcs.ITP.2023.36. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITP.2023.36.

[BS66a] A. I. Borevich and I. R. Shafarevich. *Number theory*. Pure and Applied Mathematics, Vol. 20. Academic Press, New York-London, 1966, pages x+435.

[BS66b] Z. I. Borevich and I. R. Shafarevich. *Number theory. Translated by Newcomb Greenleaf*. English. Volume 20. Pure Appl. Math., Academic Press. New York and London: Academic Press, 1966.

[Buz+22] K. Buzzard, C. Hughes, K. Lau, A. Livingston, R. Fernández Mir, and S. Morrison. “Schemes in Lean”. English. In: *Exp. Math.* 31.2 (2022), pages 355–363. ISSN: 1058-6458. DOI: 10.1080/10586458.2021.1983489.

[CT+22] J. Commelin, A. Topaz, et al. “Completion of the Liquid Tensor Experiment”. Blog-post. 2022.

[Hil98] D. Hilbert. *The theory of algebraic number fields*. Translated from the German and with a preface by Iain T. Adamson, With an introduction by Franz Lemmermeyer and Norbert Schappacher. Springer-Verlag, Berlin, 1998, pages xxxvi+350. ISBN: 3-540-62779-0. DOI: 10.1007/978-3-662-03545-0. URL: https://doi.org/10.1007/978-3-662-03545-0.

[Kum50a] E. Kummer. “Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda-3)$ Bernoullischen Zahlen als Factoren nicht vorkommen.” German. In: *J. Reine Angew. Math.* 40 (1850), pages 131–138. ISSN: 0075-4102. URL: https://eudml.org/doc/147443.

[Kum50b] E. Kummer. “Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus ...ten Wurzeln der Einheit gebildeten complexen Zahlen.” ger. In: *Journal für die reine und angewandte Mathematik* 40 (1850), pages 117–129. URL: http://eudml.org/doc/147442.

[LM20] R. Y. Lewis and P. Madelaine. "Simplifying Casts and Coercions". In: *Practical Aspects of Automated Reasoning, PAAR 2020*. arXiv:2001.10594. 2020. arXiv: 2001.10594. URL: https://arxiv.org/abs/2001.10594.

[Liv23] A. Livingston. "Group Cohomology in the Lean Community Library". In: *14th International Conference on Interactive Theorem Proving (ITP 2023)*. Edited by A. Naumowicz and R. Thiemann. Volume 268. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023, 22:1–22:17. ISBN: 978-3-95977-284-6. DOI: 10.4230/LIPIcs.ITP.2023.22. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITP.2023.22.

[mat20] The mathlib Community. "The Lean Mathematical Library". In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*. CPP 2020. New Orleans, LA, USA: Association for Computing Machinery, Jan. 2020, 367–381. DOI: 10.1145/3372885.3373824. URL: https://doi.org/10.1145/3372885.3373824.

[Nar23] A. Narayanan. *Formalization of p-adic L-functions in Lean 3*. arXiv:2302.14491. 2023. URL: https://arxiv.org/abs/2302.14491.

[Oos07] R. Oosterhuis. "Mechanised theorem proving: exponents 3 and 4 of Fermat's last theorem using Isabelle". Master's Thesis. 2007. URL: fse.studenttheses.ub.rug.nl/8392/.

[Rob] X.-F. Roblot. "Formalizing the analytic class number formula in Lean". In preparation.

[SD01] H. P. F. Swinnerton-Dyer. *A brief guide to algebraic number theory*. Volume 50. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 2001, pages x+146. ISBN: 0-521-00423-3. DOI: 10.1017/CBO9781139173360. URL: https://doi.org/10.1017/CBO9781139173360.

[TW95] R. Taylor and A. Wiles. "Ring-theoretic properties of certain Hecke algebras". In: *Ann. of Math. (2)* 141.3 (1995), pages 553–572. ISSN: 0003-486X. DOI: 10.2307/2118560. URL: https://doi.org/10.2307/2118560.

[Was97] L. C. Washington. *Introduction to cyclotomic fields*. Second. Volume 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, pages xiv+487. ISBN: 0-387-94762-0.

[Wie23] E. Wieser. “Multiple-Inheritance Hazards in Dependently-Typed Algebraic Hierarchies”. In: *Intelligent Computer Mathematics*. Edited by C. Dubois and M. Kerber. arXiv:2306.00617. Cham: Springer Nature Switzerland, 2023, pages 222–236. ISBN: 978-3-031-42753-4.

[Wil95] A. Wiles. “Modular elliptic curves and Fermat’s last theorem”. In: *Ann. of Math. (2)* 141.3 (1995), pages 443–551. ISSN: 0003-486X. DOI: 10.2307/2118559. URL: https://doi.org/10.2307/2118559.