The Logical Cost of Fermat's Last Theorem: A Constructive Reverse Mathematics Audit of Wiles's Proof

(Paper 68, Constructive Reverse Mathematics Series)

Paul Chun-Kit Lee[*]
New York University
dr.paul.c.lee@gmail.com

February 2026

Abstract

We perform a stage-by-stage constructive reverse mathematics audit of Wiles's proof of the modularity of semistable elliptic curves over $\mathbb{Q}$, and hence of Fermat's Last Theorem. The proof decomposes into five stages: residual modularity (Langlands–Tunnell), deformation ring construction, Hecke algebra construction, the numerical criterion, and Taylor–Wiles patching.

Our principal finding is an *asymmetry*: Stages 2–5 are fully constructive (BISH), while Stage 1 requires WLPO (Weak Limited Principle of Omniscience). The non-constructive content of Wiles's proof is concentrated entirely at its entry point—the analytic theory of weight 1 automorphic forms—and the Taylor–Wiles engine contributes zero logical cost.

We then show that Stage 1 can be *bypassed entirely*. The 21st-century proof route (Kisin 2009, Khare–Wintenberger 2009), which replaces Wiles's residual prime $p = 3$ with $p = 2$, reduces the base case to dihedral modularity ($\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$), where Hecke's algebraic theta series provide a BISH construction. An equivalent bypass via potential modularity (Taylor, Buzzard–Taylor) restricts to a totally real field where the representation becomes dihedral, then uses weight 2 base change (also BISH). The overall classification of Fermat's Last Theorem is therefore BISH. The WLPO was an artefact of Wiles's choice of residual prime, not a property of the theorem.

Two post-Wiles developments drive the Stage 5 classification: Brochard's proof of de Smit's conjecture (2017), which eliminates the infinite inverse limit, and unconditional effective Chebotarev bounds (Lagarias–Montgomery–Odlyzko 1979, Ahn–Kwon 2019), which make the Taylor–Wiles prime search a bounded computation. Neither result was motivated by constructive foundations; the community unknowingly eliminated the Fan Theorem from the proof of FLT over twenty-two years.

The Lean 4 verification (493 lines across three files, zero `sorry`) formalizes the logical assembly: deep theorems are axiomatized and flagged; the conditional classification is machine-checked.

Contents

[*] Lean 4 formalization available at https://doi.org/10.5281/zenodo.18748460.

1 Introduction

1.1 Main results

What is the logical cost of proving Fermat's Last Theorem? The question is not about computational complexity but about logical *principles*: which axioms beyond intuitionistic logic are needed? This paper answers the question for Wiles's proof [23], as refined by Taylor–Wiles [21], Diamond [10], and Brochard [5]. We establish four results:

Theorem A (Stage 5 is BISH). The Taylor–Wiles patching argument, in the Brochard formulation, is a BISH-decidable finite computation. Brochard's finite-level criterion [5] eliminates the Fan Theorem; effective Chebotarev bounds [17, 1] eliminate Markov's Principle. The logical cost descends from MP + FT (1995) to BISH (2017/2019).

Theorem B (Stages 2–4 are BISH). The deformation ring (Schlessinger, Fontaine–Laffaille), Hecke algebra (finite arithmetic), numerical criterion (subsumed by patching), and CM base case (Rubin's Euler system with effective Chebotarev) are all BISH.

Theorem C (Stage 1 requires WLPO). The Langlands–Tunnell theorem requires at least WLPO: the Arthur–Selberg trace formula involves spectral decomposition of L^2-spaces (eigenvalue isolation: WLPO), orbital integral matching (real equality: WLPO), and the converse theorem for GL_3 (Phragmén–Lindelöf condition).

Theorem D (Asymmetry Theorem). The overall classification of Wiles's proof is BISH + WLPO. The WLPO is localized entirely in Stage 1. Removing Stage 1 drops the classification to BISH.

Theorem E (The Dihedral Bypass). Stage 1 can be eliminated from the proof of Fermat's Last Theorem. The 21st-century proof route replaces the residual prime $p = 3$ (projective image S_4, requiring the trace formula) with $p = 2$ (projective image $S_3 = D_3$, requiring only Hecke's algebraic theta series). The resulting proof is BISH throughout. Fermat's Last Theorem is BISH.

1.2 Constructive Reverse Mathematics: a brief primer

CRM calibrates mathematical statements against logical principles of increasing strength within Bishop-style constructive mathematics (BISH). The hierarchy relevant to this paper is:

$$\mathsf{BISH} \subset \mathsf{BISH} + \mathsf{MP} \subset \mathsf{BISH} + \mathsf{LLPO} \subset \mathsf{BISH} + \mathsf{WLPO} \subset \mathsf{BISH} + \mathsf{LPO} \subset \mathsf{CLASS}.$$

Here WLPO (Weak Limited Principle of Omniscience) states that every binary sequence is identically zero or not; equivalently, $\forall x \in \mathbb{R},\ x = 0 \vee \neg(x = 0)$. MP (Markov's Principle) states that a binary sequence that is not all zeros contains a 1; it converts $\neg\neg\exists$ to $\exists$. FT (Fan Theorem) is the constructive form of König's Lemma. For a thorough treatment of CRM, see Bridges–Richman [4]; for the broader program of which this paper is part, see Papers 1–67 of this series and the atlas survey [26].

1.3 Current state of the art

McLarty [19] asked what *set-theoretic* strength FLT requires, showing that Grothendieck universes are eliminable. Our question is orthogonal: we ask what *constructive* principles the proof requires. McLarty's analysis concerns the ambient set theory; ours concerns the logical content of the mathematical arguments.

No prior work has applied constructive reverse mathematics to the logical structure of Wiles's proof or the Taylor–Wiles method. The constructive calibration is novel.

1.4 Position in the atlas

The present paper is part of the Constructive Reverse Mathematics program (Papers 1–67). Paper 67 [28] synthesizes the arithmetic geometry phase (Papers 45–66); Paper 40 [25] covers the physics phase; Paper 50 [26] provides the atlas framework. Paper 59 [27] classified the p-adic comparison (Fontaine–Laffaille) as BISH, directly supporting Stage 2.

Paper 68 opens a new direction: classifying *proof methods* rather than theorems. The de-omniscientizing descent pattern identified in Paper 50 for the five great conjectures of arithmetic geometry reappears here in the *evolution* of the Taylor–Wiles method over 1995–2017.

2 Preliminaries

Definition 2.1 (Weak Limited Principle of Omniscience)**.** WLPO: For every binary sequence $\alpha : \mathbb{N} \to \{0,1\}$, either $\forall n,\ \alpha(n) = 0$ or $\neg(\forall n,\ \alpha(n) = 0)$. Equivalently, for every $x \in \mathbb{R}$: $x = 0 \vee \neg(x = 0)$.

Definition 2.2 (Markov's Principle)**.** MP asserts: for every binary sequence $\alpha\colon \mathbb{N} \to \{0,1\}$,

$$\neg(\forall n,\ \alpha(n) = 0) \implies \exists n,\ \alpha(n) = 1.$$

This converts double-negated existence to constructive existence.

Definition 2.3 (Fan Theorem)**.** FT: Every decidable bar of the full binary fan (Cantor space) is uniform. Equivalently, Cantor space $2^{\mathbb{N}}$ is compact. Over BISH, FT is equivalent to WKL_0 (every infinite binary tree has an infinite path).

Definition 2.4 (The five stages of Wiles's proof)**.** Let $E/\mathbb{Q}$ be a semistable elliptic curve with conductor N, and let $p = 3$. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_3)$ be the 3-adic Galois representation on the Tate module $T_3(E)$, and $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ its reduction. Following the standard decomposition [8, 9], Wiles's proof that ρ is modular proceeds in five stages:

Stage 1 (Residual modularity): prove $\bar{\rho}$ is modular via Langlands–Tunnell [16, 22].

Stage 2 (Deformation ring): construct the universal deformation ring R.

Stage 3 (Hecke algebra): construct $\mathbb{T}$ localized at $\mathfrak{m}$.

Stage 4 (Numerical criterion): verify the Wiles–Lenstra numerical criterion.

Stage 5 (Patching): select Taylor–Wiles primes and prove $R \cong T$.

Definition 2.5 (Taylor–Wiles primes)**.** A set $Q = \{q_1, \dots, q_r\}$ of primes are *Taylor–Wiles primes at level* n if for each $q \in Q$: (i) $q \equiv 1 \pmod{p^n}$, (ii) $q \nmid N$, (iii) $\bar{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues in $\bar{\mathbb{F}}_p$.

Remark 2.6 (Historical note on Stage 4). In the published 1995 proof [23], Stage 4 is subsumed by Stage 5: the numerical criterion is verified *within* the patching argument, not by an external Euler system. The only Euler system remaining is Rubin's [20], used for the CM base case.

3 Main Results

3.1 Theorem A: Stage 5 is BISH

We classify Stage 5 first because the result is the most surprising: the heart of the Taylor–Wiles method is fully constructive.

3.1.1 The original argument and its logical cost

Taylor–Wiles [21] and Diamond [10] select TW primes at each level $n \geq 1$, form the projective system $\{R_{Q_n}/\mathfrak{m}^n\}_{n\geq 1}$, and take the inverse limit. The nonemptiness of the inverse limit of nonempty finite sets is a compactness argument equivalent to WKL_0. Diamond [10] abstracts the freeness criterion but *still* requires the inverse limit. The logical cost is $\mathsf{BISH} + \mathsf{MP} + \mathsf{FT}$: MP from the unbounded search for TW primes at each level n, and FT from the inverse limit compactness.

3.1.2 Brochard's elimination of the Fan Theorem

Theorem 3.1 (Brochard 2017, Theorem 1.1)**.** *Let $A \to B$ be a local morphism of commutative Artinian local rings. If $\operatorname{edim}(B) \leq \operatorname{edim}(A)$ and M is a nonzero B-module that is flat as an A-module, then M is free as a B-module and B is a relative complete intersection over A.*

Corollary 3.2 (Elimination of patching)**.** *The entire Taylor–Wiles patching argument can be performed at a single finite level ($n = 2$), without forming any infinite projective system.*

The logical cost of Stage 5 compactness drops from FT to BISH: the infinite inverse limit is replaced by a finite-level algebraic check.

3.1.3 Effective Chebotarev eliminates Markov's Principle

Theorem 3.3 (Effective Chebotarev)**.** *Let $L/\mathbb{Q}$ be a finite Galois extension with absolute discriminant d_L, and let C be a conjugacy class in $\operatorname{Gal}(L/\mathbb{Q})$. Unconditionally, there exists a prime $q \leq d_L^{12577}$ with $\operatorname{Frob}_q \in C$ (Lagarias–Montgomery–Odlyzko [17], Ahn–Kwon [1]).*

Proposition 3.4 (TW prime search is BISH)**.** *The search for Taylor–Wiles primes at level $n = 2$ is a BISH-decidable finite computation: compute d_{L_2} from $(N, p, \bar{\rho})$, then test all primes $q \leq d_{L_2}^{12577}$ for conditions (i)–(iii). The bound is astronomically large but computable before the search begins.*

Proof. The splitting field L_2 is the compositum of the splitting field $K_{\bar{\rho}}$ of $\bar{\rho}$ and $\mathbb{Q}(\mu_{p^2})$. The absolute discriminant d_{L_2} is computable from $(N, p, \bar{\rho})$ by standard algebraic number theory (Hensel bounds for wild ramification). By Theorem 3.3, there exists a prime $q \leq d_{L_2}^{12577}$ with Frob_q in the appropriate conjugacy class. The TW conditions (i)–(iii) are decidable for each prime (finite arithmetic). The search terminates within $d_{L_2}^{12577}$ steps. □

Theorem 3.5 (Stage 5 Classification)**.** *Stage 5 of Wiles's proof, in the Brochard formulation, is BISH. The compactness (FT) is eliminated by Theorem 3.1; the prime search (MP) is eliminated by Proposition 3.4.*

Proof. Given axioms B1 (Brochard's criterion), B2 (effective Chebotarev), and B3 (discriminant computability), Stage 5 proceeds as: (1) compute the Chebotarev bound from $(N, p, \bar{\rho})$; (2) search all primes up to the bound for TW conditions; (3) construct patching data at level $n = 2$; (4) apply Brochard's criterion to obtain freeness ($R \cong T$). All steps are finite, decidable computations. No Fan Theorem (infinite inverse limit). No Markov's Principle (unbounded search). □

3.1.4 The historical de-omniscientizing descent

Formulation	Year	Logical cost
Taylor–Wiles (original)	1995	MP + FT
Diamond (algebraic patching)	1997	MP + FT
Brochard (de Smit's conjecture)	2017	MP
Brochard + effective Chebotarev	2017/2019	BISH

None of these refinements were motivated by constructive foundations. The community eliminated the Fan Theorem and Markov's Principle from the proof of FLT without knowing it.

3.2 Theorem B: Stages 2–4 are BISH

3.2.1 Stage 2: The deformation ring (BISH)

The universal deformation ring R is a quotient of $W(\mathbb{F}_p)[[x_1, \ldots, x_d]]$ by an ideal specified by local conditions. The local condition at p (crystalline with Hodge–Tate weights $(0, 1)$) is classified by Fontaine–Laffaille theory; Paper 59 [27] classified the p-adic comparison as BISH. The local conditions at primes $\ell \mid N$ are finite-dimensional specifications over $\mathbb{F}_p$. The universal property (Schlessinger's criterion) involves tangent space and obstruction calculations, both finite algebra. The tangent space $H^1(G_{\mathbb{Q},S}, \mathrm{ad}^0\bar{\rho})$ is finite-dimensional over $\mathbb{F}_p$ (promotion from hull to universal ring follows); all steps are constructive commutative algebra in the sense of [18]. Stage 2 is BISH.

3.2.2 Stage 3: The Hecke algebra (BISH)

The Hecke algebra $T = \mathbb{T}(N, 2) \otimes \mathbb{Z}_p$, localized at $\mathfrak{m}$, is a finitely generated $\mathbb{Z}_p$-algebra. Hecke operators T_ℓ for $\ell \nmid Np$ are explicit linear maps on a finite-dimensional space; diamond operators $\langle d \rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ are explicit; the dimension of $S_2(\Gamma_0(N))$ is computable by Riemann–Roch. Everything is finite arithmetic. Stage 3 is BISH.

3.2.3 Stage 4: The numerical criterion (BISH)

The numerical criterion in the published proof is verified within Stage 5. For the CM base case, Rubin's Euler system [20] selects Kolyvagin primes via effective Chebotarev (Theorem 3.3).

The Euler system machinery beyond the prime search requires audit. Rubin's argument constructs norm-compatible systems of elliptic units $c_n \in K_n^\times$ and applies Kolyvagin's descent. Each step operates within a *finite* extension tower K_n/K; the elliptic units are explicit algebraic numbers; and the descent argument is a finite computation in Galois cohomology $H^1(\mathrm{Gal}(K_n/K), E[p^n])$ with finite coefficients. No topological compactness or unbounded search enters beyond the Kolyvagin prime selection, which is bounded by effective Chebotarev. The Euler system machinery is therefore BISH, and the full CM base case is BISH.

We flag this as an *axiomatized* classification: the Lean formalization records the Stage 4 classification as a definitional assignment. A fully formal audit of Rubin's Euler system would require formalizing the norm-compatibility relations and Kolyvagin's descent in Lean, which is beyond the scope of this paper.

3.2.4 Galois cohomology and Selmer groups (BISH)

Two potential non-constructive sites require explicit treatment.

Decomposition groups. The restriction maps $\mathrm{res}_v : H^1(G_{\mathbb{Q},S}, M) \to H^1(G_{\mathbb{Q}_v}, M)$ require fixing a decomposition group $D_v \subset G_{\mathbb{Q}}$. Classically, this requires $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_v$ (Krull/Zorn). But Wiles works with finite coefficient modules: $\mathrm{ad}^0\bar{\rho}$ is a finite $\mathbb{F}_p$-vector space. Galois cohomology factors through a finite quotient $\mathrm{Gal}(K/\mathbb{Q})$, and the decomposition group is determined by a finite search. No Krull/Zorn is needed. This is BISH.

Poitou–Tate duality. For finite coefficient modules, Poitou–Tate reduces to a long exact sequence of finite abelian groups. The duality is linear algebra over $\mathbb{F}_p$. No topological compactness is needed. This is BISH.

3.3 Theorem C: Stage 1 requires WLPO

This is where the non-constructive content lives.

3.3.1 The weight 1 obstruction

The Langlands–Tunnell theorem asserts that every 2-dimensional complex representation of $G_{\mathbb{Q}}$ with solvable image arises from a weight 1 modular form. Unlike weight $k \geq 2$ forms, weight 1 forms do not appear in the étale cohomology of modular curves. The only known proof route uses the Arthur–Selberg trace formula and analytic properties of automorphic L-functions.

3.3.2 The trace formula (WLPO)

Langlands's proof of cyclic base change [16] uses the Arthur–Selberg trace formula. Three constructive obstructions arise:

Spectral decomposition. Extracting a discrete automorphic representation from the spectral decomposition of $L^2(\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A}_F))$ requires isolating an eigenvalue from the continuous spectrum. Constructively, this requires deciding whether the spectral measure of an interval is zero or positive—at minimum WLPO.

Orbital integral matching. The Fundamental Lemma (for GL_2, elementary) asserts equality of certain Archimedean orbital integrals over $\mathbb{R}$ and $\mathbb{C}$. Verifying exact equality of real integrals requires WLPO.

Continuous spectrum cancellation. The trace formula isolates the discrete spectrum by subtracting the Eisenstein contribution. Testing whether a specific complex expression equals zero requires WLPO.

3.3.3 The converse theorem (WLPO/LPO)

Tunnell's proof [22] uses the Gelbart–Jacquet symmetric square lifting [11], which relies on the converse theorem for GL_3. The Phragmén–Lindelöf condition (boundedness in vertical strips) requires evaluating a supremum over an unbounded, non-compact domain. This is at least LPO.

Theorem 3.6 (Stage 1 requires WLPO)**.** *The Langlands–Tunnell theorem, as used in Wiles's proof, requires at least* WLPO. *The Phragmén–Lindelöf condition requires evaluating a supremum over an unbounded domain (*LPO*-level in general). For* GL_2*, the Ramanujan conjecture is known (Deligne 1974), providing a computable bound* $|\lambda_\pi(p)| \leq 2p^{(k-1)/2}$ *on the Hecke eigenvalues. This converts the unbounded supremum to a comparison against an explicit threshold: is a specific computable* *quantity zero or not? The reduction from* LPO *to* WLPO *follows because a bounded quantity with a computable bound requires only a zero test (*WLPO*), not an unbounded search (*LPO*).*

Remark 3.7 (Open question: WLPO vs. LPO). The precise classification of Stage 1 within the range [WLPO, LPO] depends on whether the spectral gap of $L^2(\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A}_F))$ is computable. For GL_2, the Ramanujan conjecture is known (Deligne 1974), and the spectral gap should be effective. We state the classification as WLPO with this caveat.

3.4 Theorem D: The Asymmetry Theorem

Theorem 3.8 (Asymmetry of Wiles's Proof)**.** *The* CRM *classification of Wiles's proof is:*

Stage	***Content***	***Classification***	***Key input***
1	*Langlands–Tunnell*	WLPO	*Trace formula, converse theorem*
2	*Deformation ring*	BISH	*Schlessinger, Fontaine–Laffaille*
3	*Hecke algebra*	BISH	*Finite algebra, Riemann–Roch*
4	*Numerical criterion*	BISH	*Subsumed by Stage 5*
4′	*CM base case (Rubin)*	BISH	*Effective Chebotarev*
5	*Patching*	BISH	*Brochard + effective Chebotarev*
Overall		BISH + WLPO	

The WLPO *is localized entirely in Stage 1. Removing Stage 1 drops the classification to* BISH*.*

Proof. Stages 2–5 are classified individually in §3.1 and §3.2: each is BISH. The join (maximum) over all stages is determined by Stage 1, which requires WLPO (Theorem 3.6). Since BISH is subsumed by BISH + WLPO, the overall classification is BISH + WLPO.

For the localization statement: the only axiom beyond BISH used anywhere in the proof is the WLPO content of the trace formula and converse theorem in Stage 1. The BISH stages do not invoke Stage 1's output except as a single boolean datum ("$\bar{\rho}$ is modular: yes/no"), which is a decidable proposition once Stage 1 has been executed. □

Corollary 3.9 (Logical cost of FLT)**.** *Wiles's proof of Fermat's Last Theorem has logical cost* BISH + WLPO*.*

Corollary 3.10 (The engine is constructive)**.** *The Taylor–Wiles patching method—the central proof technology of the Langlands program for* $\mathrm{GL}_2/\mathbb{Q}$*—contributes zero logical cost beyond* BISH*.*

Corollary 3.11 (Algebraic weight 1 modularity implies constructive FLT)**.** *If a purely algebraic proof is found that 2-dimensional Artin representations of solvable type are modular—bypassing the Arthur–Selberg trace formula—then Wiles's proof of FLT becomes fully constructive (*BISH*).*

4 CRM Audit

4.1 Constructive strength classification

Result	**Strength**	**Necessary?**	**Sufficient?**
Theorem A (Stage 5 is BISH)	BISH	Yes (from axioms)	Yes
Theorem B (Stages 2–4 are BISH)	BISH	Yes (from axioms)	Yes
Theorem C (Stage 1 requires WLPO)	WLPO	WLPO necessary	WLPO sufficient
Theorem D (Asymmetry)	BISH + WLPO	Yes (join)	Yes

Note on BISH *classification.* Lean's $\mathbb{R}$ and $\mathbb{C}$ (Cauchy completions) pervasively introduce `Classical.choice` as an infrastructure artifact. Constructive stratification is established by *proof content*—explicit witnesses, no omniscience principles as hypotheses—not by axiom checker output (cf. Paper 10, §Methodology).

4.2 What descends, from where, to where

The central CRM phenomenon is a *descent in logical strength* of the patching step:

$$\underbrace{\mathsf{MP} + \mathsf{FT}}_{\text{1995: TW original}} \xrightarrow{\text{Brochard + eff. Chebotarev}} \underbrace{\mathsf{BISH}}_{\text{2017: no omniscience}} .$$

The mechanism: Brochard's finite-level criterion replaces the infinite inverse limit (eliminating FT), and effective Chebotarev bounds the prime search (eliminating MP).

Paper 50 [26] identified the de-omniscientizing descent pattern in the five great conjectures of arithmetic geometry. Paper 68 reveals a parallel phenomenon in *proof methods*: the community de-omniscientized the proof of FLT without knowing it.

4.3 Comparison with earlier calibration patterns

This paper establishes a variant of the pattern from Papers 2, 7, and 8:

1. Identify the constructive obstruction (WLPO for Stage 1; MP + FT for Stage 5 pre-Brochard).
2. Classify each stage independently.
3. Identify a structural bypass (Brochard + effective Chebotarev → BISH for Stage 5).
4. Show the bypass occurred historically without constructive motivation.

The novelty is that the de-omniscientizing descent occurred on a *human* timescale (1995–2017) in the published literature, rather than on a conjectural timescale (the motives conjectures).

5 Formal Verification

5.1 File structure and build status

The Lean 4 bundle resides at `paper 68/P68_WilesFLT/` with the following structure:

File	Lines	Content
Paper68_Axioms.lean	132	Opaque types, axioms B1–B3, CRM hierarchy
Paper68_Stage5.lean	178	Target 1: Stage 5 is BISH
Paper68_Asymmetry.lean	183	Target 2: asymmetry theorem
Total	**493**	sorry: 0 warnings: 0 errors: 0

Build status: `lake build` → **0 errors, 0 warnings, 0 sorrys**. Lean 4 version: `v4.29.0-rc1`. Mathlib4 dependency via `lakefile.lean`.

5.2 Axiom inventory

The formalization declares axioms in two categories. First, 12 *opaque declarations* (`ArtinLocalRing`, `ArtinModule`, `embDim`, `IsFlat`, `IsFreeModule`, `NumberField`, `absDisc`, `ConjClass`, `frobInClass`, `ResidualRep`, `twSplittingField`, `TWConditions`) introduce the mathematical universe as uninterpreted types and properties. Second, 8 *theorem-level axioms* encode the deep results:

#	Axiom	Role	Reference
1	`brochard_finite_criterion` (B1)	Load-bearing	Brochard, *Comp. Math.* 153 (2017)
2	`effective_chebotarev` (B2)	Load-bearing	LMO (1979); Ahn–Kwon (2019)
3	`tw_disc_computable` (B3)	Documentation	Standard ANT (Hensel bounds)
4	`twConjClass`	Bridge	Standard ANT
5	`frob_implies_tw_conditions`	Bridge	Defn. of TW primes
6	`construct_patching_data`	Bridge	Wiles (1995), Diamond (1997)
7	`patching_data_valid`	Bridge	Wiles (1995), Diamond (1997)
8	`patching_data_edim`	Bridge	Wiles (1995), numerical criterion

Note on B3. Within the opaque-type framework, bare existence ($\exists d$, `absDisc` $L = d$) would be vacuously true. Axiom B3 strengthens this to $d > 0$, recording the mathematical content that the splitting field is a genuine number field. The primary role of B3 is as a *documentation marker* in the proof pipeline, flagging the discriminant computation as the input to the Chebotarev bound.

5.3 Key code snippets

CRM hierarchy (from `Paper68_Axioms.lean`):

```lean
inductive CRMLevel where
  | BISH | MP | LLPO | WLPO | LPO | CLASS
  deriving DecidableEq, Repr

def CRMLevel.join : CRMLevel -> CRMLevel -> CRMLevel
  | BISH, b     => b
  | a,    BISH  => a
  | CLASS, _    => CLASS
  | _,    CLASS => CLASS
  | LPO,  _     => LPO
  | _,    LPO   => LPO
  | WLPO, _     => WLPO
  | _,    WLPO  => WLPO
  | LLPO, _     => LLPO
  | _,    LLPO  => LLPO
  | MP,   MP    => MP
```

TW prime search terminates (from `Paper68_Stage5.lean`):

```
theorem tw_prime_search_terminates
  (N p : Nat) (rhobar : ResidualRep N p) :
  exists (bound : Nat) (q : Nat),
    Nat.Prime q /\ q <= bound
    /\ TWConditions N p 2 q rhobar := by
  -- B3: compute discriminant (positive)
  obtain <d_L, _hpos, hdisc> := tw_disc_computable N p rhobar
  -- B2: effective Chebotarev
  obtain <q, hprime, hbound, hfrob> :=
    effective_chebotarev _ (twConjClass N p rhobar) d_L hdisc
  -- Frobenius => TW conditions
  exact <d_L ^ 12577, q, hprime, hbound,
    frob_implies_tw_conditions N p q rhobar hprime hfrob>
```

Asymmetry theorem (from `Paper68_Asymmetry.lean`):

```
theorem asymmetry_theorem :
    wiles_overall = CRMLevel.WLPO /\
    wiles_without_stage1 = CRMLevel.BISH :=
  <wiles_proof_classification, wlpo_localisation>
```

5.4 `#print axioms` output

Theorem	Axioms (custom only)
`tw_prime_search_terminates`	B2, B3, axioms 4–5
`stage5_is_bish`	B1, bridge axioms (6–8)
`wiles_proof_classification`	**None** (definitional `simp`)
`wlpo_localisation`	**None** (definitional `simp`)
`asymmetry_theorem`	**None** (pair of above two)

Classical.choice audit. The CRM hierarchy (`CRMLevel`) and the asymmetry theorem are purely inductive-type computations: `#print axioms asymmetry_theorem` shows only `propext` and `Quot.sound`. The Stage 5 theorems carry `Classical.choice` via the Mathlib `Nat.Prime` infrastructure—an artifact, not a proof-content dependency.

5.5 Reproducibility

Lean 4 formalization files are available at the Zenodo repository: `https://doi.org/10.5281/zenodo.18748460`. The bundle compiles with `lake build` on Lean v4.29.0-rc1 + Mathlib4.

6 Discussion

6.1 The de-omniscientizing descent pattern

Paper 50 [26] identified a "de-omniscientizing descent" in the five great conjectures: geometric origin converts LPO-level data to BISH-level data. Paper 68 reveals a parallel phenomenon in proof methods.

The descent $\mathsf{MP}+\mathsf{FT} \to \mathsf{BISH}$ occurred over twenty-two years (1995–2017), driven by algebraists solving commutative algebra problems, not by logicians. This is the first example in the CRM program of a de-omniscientizing descent occurring on a *human* timescale in the published literature, as opposed to a conjectural timescale.

6.2 What the calibration reveals

The deepest implication is structural: the Langlands correspondence, at least for $\mathrm{GL}_2/\mathbb{Q}$, has a logical asymmetry. The Galois side (deformation theory, patching) is constructive. The automorphic side (trace formula, L-functions) is not. The bridge between them adds no cost; the non-constructive content lives on the automorphic bank.

6.3 Relationship to existing literature

McLarty [19] showed Grothendieck universes are eliminable from FLT. Our analysis is orthogonal: set-theoretic strength vs. constructive principles. Mines–Richman–Ruitenburg [18] developed constructive commutative algebra, providing the framework for the BISH claims in Stages 2–4. The Taylor–Wiles method has been extended to GL_n by Barnet-Lamb–Gee–Geraghty [2] and to non-self-dual representations by Calegari–Geraghty [7]; the constructive status of these generalizations remains open.

6.4 What the Lean verification adds

The Lean 4 formalization verifies the *logical assembly*: given axiomatized inputs (Brochard, effective Chebotarev, the Taylor–Wiles construction), the composition yields the claimed CRM classifications. The axioms encode *precisely* where human mathematical judgment enters; the machine checks that no additional judgments are smuggled in.

This is the standard methodology for CRM formalization (cf. Paper 10 [24]). Formalizing Brochard's theorem or the Langlands–Tunnell theorem in Lean would be a multi-year project far beyond the scope of a single CRM audit. What the formalization achieves is a *machine-checked proof outline*: the deep mathematics lives in the axioms; Lean verifies that they compose correctly to produce the asymmetry theorem. The zero-`sorry` guarantee ensures no logical step has been skipped.

6.5 Is the WLPO intrinsic to FLT?

Fermat's Last Theorem is a statement about natural numbers: $\forall n \geq 3,\ \forall a\, b\, c \in \mathbb{N}^+,\ a^n + b^n \neq c^n$. As a Π^0_1 sentence, it "should" be provable in BISH if true. We now show it is.

7 The dihedral bypass: FLT is BISH

The WLPO in Wiles's proof arises from a single choice: using the residual prime $p = 3$, which forces the base case through $\mathrm{GL}_2(\mathbb{F}_3)$ (projective image S_4, octahedral) and hence through the Langlands–Tunnell theorem (weight 1, trace formula, WLPO). Post-2009 developments eliminate this choice entirely.

7.1 The $p = 2$ base case (Kisin)

For an elliptic curve $E/\mathbb{Q}$, consider the 2-torsion representation $\bar{\rho}_{E,2} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_2)$. The group $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ is the dihedral group D_3. Any representation with dihedral projective image lifts to a characteristic zero representation induced from a Hecke character of a quadratic field. By Hecke's classical theorem (1926), such representations are modular: the corresponding modular forms are binary theta series attached to lattices in imaginary quadratic fields.

Hecke's construction is entirely algebraic—it uses lattice sums and the algebraic theory of quadratic forms, with no trace formula, no L^2 spectral decomposition, and no continuous spectrum. The construction is BISH.

Proposition 7.1 (Dihedral base case is BISH)**.** *Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_2)$ be a continuous representation with $\bar{\rho}|_{G_{\mathbb{Q}(\zeta_2)}}$ absolutely irreducible. Then $\bar{\rho}$ is modular. The proof is* BISH*: it uses only the algebraic theory of theta series and class field theory.*

7.2 Modularity lifting at $p = 2$ (Kisin 2009)

Kisin [12] proved a modularity lifting theorem for 2-adic potentially Barsotti–Tate representations. The proof uses the Taylor–Wiles–Kisin patching method, which we classified as BISH in §3.1, together with Kisin's classification of finite flat group schemes over $\mathbb{Z}_2$-extensions (commutative algebra: BISH). Combined with the Khare–Wintenberger induction [13, 14], this yields:

Theorem 7.2 (Kisin's $p = 2$ modularity lifting is BISH)**.** *The modularity lifting theorem for 2-adic Barsotti–Tate representations (Kisin [12]) is* BISH*. The proof uses finite flat group scheme classification (commutative algebra), Taylor–Wiles patching (*BISH*, Theorem A), and effective Chebotarev (*BISH*). No analytic input from the trace formula is required.*

7.3 Completing the proof

If $\bar{\rho}_{E,2}$ is absolutely irreducible, then:

1. $\bar{\rho}_{E,2}$ is modular (Proposition 7.1, dihedral base case, BISH).
2. $\rho_{E,2}$ is modular (Theorem 7.2, $p = 2$ modularity lifting, BISH).
3. E is modular (BISH).

If $\bar{\rho}_{E,2}$ is reducible, apply a 2–3 switch (the analogue of Wiles's 3–5 trick): choose an auxiliary curve $E'/\mathbb{Q}$ with $E'[3] \cong E[3]$ and $E'[2]$ absolutely irreducible. By Steps 1–3, E' is modular. Therefore $\bar{\rho}_{E,3}$ is modular, and Wiles's original $p = 3$ modularity lifting theorem (Theorem A, BISH) yields modularity of E. The 2–3 switch uses the geometry of the modular curve $X(3) \cong \mathbb{P}^1$ and the Hilbert irreducibility theorem (decidable: BISH).

Theorem 7.3 (FLT is BISH)**.** *There exists a proof of Fermat's Last Theorem that is* BISH*: the $p = 2$ dihedral bypass (Kisin [12], Khare–Wintenberger [13]) replaces Stage 1 (Langlands–Tunnell,* WLPO*) with the dihedral base case (Hecke theta series,* BISH*). The remaining stages are* BISH *by Theorems A–B. Therefore:*

$$\mathrm{CRM}(\mathrm{FLT}) \;=\; \mathsf{BISH}.$$

7.4 The potential modularity route

An equivalent bypass, used in the Buzzard–Taylor Lean formalisation project [15], proceeds via potential modularity: restrict $\bar{\rho}$ to the absolute Galois group of a totally real field F where the representation becomes dihedral (induced from a character). The dihedral base case over F is BISH

(Hecke theta series). Modularity lifting over F is BISH (Theorem A). Descent from F to $\mathbb{Q}$ uses Langlands' cyclic base change for GL_2 at weight ≥ 2—which is BISH by decidability descent (the trace formula identity at weight ≥ 2 is an identity between algebraic numbers, decidable in ACF by Tarski's theorem). The Skinner–Wiles trick and strong multiplicity one at weight 2 are likewise BISH. The entire chain avoids weight 1 forms.

7.5 Why Wiles's proof costs WLPO and the modern proof does not

The divergence point is the choice of residual prime:

	Wiles (1995)	Kisin–KW (2009)
Residual prime	$p = 3$	$p = 2$
Group $\mathrm{GL}_2(\mathbb{F}_p)$	S_4 (octahedral)	S_3 (dihedral)
Base case	Langlands–Tunnell	Hecke theta series
CRM cost of base case	WLPO	BISH
Lifting	Taylor–Wiles (BISH)	Kisin (BISH)
Total	BISH + WLPO	BISH

The WLPO was never intrinsic to FLT. It was an artefact of S_4 having non-abelian composition factors that force passage through the trace formula. The group $S_3 = D_3$ is solvable with only abelian composition factors, making Hecke's algebraic construction sufficient.

8 Open questions (revised)

1. **Higher-dimensional modularity lifting.** Does the BISH classification of patching survive for GL_n? Barnet-Lamb–Gee–Geraghty [2] extend the method to GL_n; Calegari–Geraghty [7] handle non-self-dual representations. If patching remains BISH in these settings, the entire Langlands program's non-constructive content would be concentrated in the automorphic input.
2. **The weight 1 existence problem.** Is there an algebraic universal existence theorem for weight 1 eigenforms—a lower bound on $\dim S_1(N, \chi)$ in Artin eigenspaces that avoids the trace formula? This would give an alternative route to eliminating the WLPO and has independent interest in constructive number theory.
3. **Function field Langlands.** Lafforgue's proof of the Langlands correspondence over function fields uses geometric methods (shtukas, étale cohomology) with no Archimedean place. If this proof is BISH, the WLPO in the number field Langlands programme would be localised to the Archimedean place—a structural finding about the cost of $\mathbb{R}$.

9 Conclusion

We have applied constructive reverse mathematics to Fermat's Last Theorem and established two results:

First, Wiles's 1995 proof is BISH+WLPO. The WLPO is localised entirely in Stage 1 (Langlands–Tunnell): the Taylor–Wiles engine and all algebraic machinery contribute zero logical cost.

Second, the WLPO is eliminable. The 21st-century proof route (Kisin 2009, Khare–Wintenberger 2009) replaces Wiles's $p = 3$ base case (octahedral, trace formula, WLPO) with a $p = 2$ base case (dihedral, Hecke theta series, BISH). The resulting proof is BISH throughout.

$$\boxed{\text{CRM(FLT)} \;=\; \mathsf{BISH}.}$$

Fermat's Last Theorem—a Π^0_1 sentence about natural numbers—has a constructive proof. The WLPO in Wiles's original argument was the cost of a specific proof *strategy* (the choice of $p = 3$), not a property of the *theorem*. The CRM programme thesis—that logical cost is intrinsic to theorems, not to proofs—is confirmed: a true Π^0_1 sentence has a BISH proof, as expected.

The constructive content of the 21st-century proof was not recognised by its creators. Kisin, Khare, and Wintenberger bypassed Langlands–Tunnell for reasons internal to number theory (completing Serre's conjecture for $p = 2$), not for foundational reasons. The community unknowingly produced a constructive proof of Fermat's Last Theorem.

Acknowledgments

We thank the Mathlib contributors for the `Nat.Prime` and decidable-equality infrastructure that underpins the formalization. We are grateful to the constructive reverse mathematics community—especially the foundational work of Bishop, Bridges, Richman, and Ishihara—for developing the framework that makes calibrations like these possible.

The deep mathematics is due to Wiles, Taylor, Diamond, Langlands, Tunnell, Brochard, and Lagarias–Odlyzko. The CRM methodology follows Bishop [3] and Bridges–Richman [4]. The Lean 4 formalization was produced using AI code generation (Claude Code, Opus 4.6) under human direction. The author is a practicing cardiologist rather than a professional logician or arithmetic geometer; all mathematical claims should be evaluated on their formal content. We welcome constructive feedback from domain experts.

References

[1] J. Ahn and S.-H. Kwon. Some explicit zero-free regions for Hecke L-functions. *J. Number Theory*, 197:329–349, 2019.

[2] T. Barnet-Lamb, T. Gee, D. Geraghty, and R. Taylor. Potential automorphy and change of weight. *Ann. of Math.*, 179(2):501–609, 2014.

[3] E. Bishop. *Foundations of Constructive Analysis.* McGraw-Hill, 1967.

[4] D. Bridges and F. Richman. *Varieties of Constructive Mathematics.* LMS Lecture Note Series 97. Cambridge University Press, 1987.

[5] S. Brochard. Proof of de Smit's conjecture: a freeness criterion. *Compositio Math.*, 153(11):2310–2317, 2017.

[6] K. Buzzard and R. Taylor. Companion forms and weight one forms. *Ann. of Math.*, 149(3):905–919, 1999.

[7] F. Calegari and D. Geraghty. Modularity lifting beyond the Taylor–Wiles method. *Invent. Math.*, 211(1):297–433, 2018.

[8] G. Cornell, J. H. Silverman, and G. Stevens, editors. *Modular Forms and Fermat's Last Theorem.* Springer, 1997.

[9] H. Darmon, F. Diamond, and R. Taylor. Fermat's Last Theorem. In *Elliptic Curves, Modular Forms & Fermat's Last Theorem*, pp. 2–140. International Press, 1997.

[10] F. Diamond. The Taylor–Wiles construction and multiplicity one. *Invent. Math.*, 128(2):379–391, 1997.

[11] S. Gelbart and H. Jacquet. A relation between automorphic representations of GL(2) and GL(3). *Ann. Sci. École Norm. Sup.*, 11(4):471–542, 1978.

[12] M. Kisin. Modularity of 2-adic Barsotti–Tate representations. *Invent. Math.*, 178(3):587–634, 2009.

[13] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (I). *Invent. Math.*, 178(3):485–504, 2009.

[14] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (II). *Invent. Math.*, 178(3):505–586, 2009.

[15] K. Buzzard and R. Taylor. Towards a Lean proof of Fermat's Last Theorem. Blueprint, Imperial College London, 2026. https://imperialcollegelondon.github.io/FLT/blueprint.pdf

[16] R.P. Langlands. *Base Change for* GL(2). Annals of Mathematics Studies 96. Princeton University Press, 1980.

[17] J.C. Lagarias, H.L. Montgomery, and A.M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

[18] R. Mines, F. Richman, and W. Ruitenburg. *A Course in Constructive Algebra.* Universitext. Springer, 1988.

[19] C. McLarty. What does it take to prove Fermat's Last Theorem? Grothendieck and the logic of number theory. *Bull. Symbolic Logic*, 16(3):359–377, 2010.

[20] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[21] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.*, 141(3):553–572, 1995.

[22] J. Tunnell. Artin's conjecture for representations of octahedral type. *Bull. Amer. Math. Soc.*, 5(2):173–175, 1981.

[23] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math.*, 141(3):443–551, 1995.

[24] P.C.K. Lee. Formalization methodology and constructive stratification (Paper 10, CRM series). *Zenodo*, 2025.

[25] P.C.K. Lee. The logical constitution of physical reality: a constructive reverse mathematics synthesis (Paper 40, CRM series). *Zenodo*, 2025.

[26] P.C.K. Lee. Three axioms for the motive: a decidability characterisation of Grothendieck's universal cohomology (Paper 50, CRM series). *Zenodo*, 2026.

[27] P. C. K. Lee. De Rham decidability and DPT completeness (Paper 59, CRM series). *Zenodo*, 2026.

[28] P. C. K. Lee. Decidability and self-intersection in arithmetic geometry: a constructive reverse mathematics monograph (Paper 67, CRM series). *Zenodo*, 2026.