

Linchpin Theorems

Abstract

A proof assistant checks a formal proposition. It does not check that the proposition expresses the mathematics that its author intended. This distinction becomes pressing when large bodies of mathematics are autoformalized. We propose the use of *linchpin theorems*: statements whose meanings can be audited with relatively little mathematical infrastructure, and whose proofs connect them to substantial results. Examples range from sphere packing and the classification of Lie algebras to regularity theory, the Weil conjectures, and computational complexity. Some linchpins are equivalent reformulations. Others are consequences, or stronger conjectures. We specify the direction of each implication and the background theorems used in the connection. A linchpin is an instrument of audit, not an end in itself. A proof that bypasses the mathematics under audit can expose a weakness of the instrument.

1 Introduction

The conclusion of a long formal proof can be difficult to read. A theorem about varieties, manifolds, or automorphic representations may depend for its meaning on hundreds of definitions. A human auditor who wishes to know whether an autoformalization has proved the intended theorem must look beyond the final line. The definitions, conventions, and hypotheses are part of the claim.

A small trusted kernel addresses a different problem. It checks that the formal conclusion follows from the formal premises. It cannot determine whether a definition of a smooth variety, a packing, or a computation captures the intended concept. A translation error may leave a well-typed, provable proposition. Autoformalization therefore increases the value of statements whose mathematical meanings are easy to inspect. Pollack [53] makes this distinction between checking a derivation and understanding the informal meaning of its conclusion.

We call such a statement a *linchpin* when it is chosen to audit a specified body of mathematics. A useful linchpin has a short statement, few prerequisites for understanding that statement, and a documented connection with the theorem under audit. It may involve only finite counting or polynomial equations. These are useful features, not requirements. An intelligible statement about continuous maps may serve better than an opaque encoding by natural numbers.

The intended arrangement is as follows. A substantial theorem T is formalized, and a statement L is derived from it. A human checks the meaning of L , while the proof assistant checks its derivation from T and the supporting library. The bridge from T to L must itself be included in the formal development. This reduces the amount of specialized language at the point of human inspection. It does not eliminate the need to examine premises, axioms, or dependencies.

Autoformalization by language models is already an active subject [68]. Our concern here is the mathematical interface presented to an auditor, independently of the method used to produce the formal text.

We use the word *linchpin* informally. It describes a role in an audit, not a new logical property of propositions. In particular, a consequence does not recover all the content of its source. Several consequences may be needed to test different parts of a development. Nor does a citation establish

that a theorem is indispensable to a proof. A published proof may use a theorem that another proof avoids.

Linchpins are not ends in themselves. Suppose that a proposed linchpin for a deep theorem acquires a proof that bypasses that theorem, whether by a human argument or by autoformalization. The new proof may be valuable mathematics. For the proposed audit, however, it shows that the linchpin did not serve its purpose. One should then seek a better linchpin. It would be a mistake to protect the choice of statement at the expense of the purpose for which it was chosen.

There are four kinds of connection in this paper. An *equivalent reformulation* satisfies $T \iff L$, using specified background results. A *downstream consequence* satisfies $T \implies L$; we make no converse claim. A *stronger conjectural formulation* implies the conjecture under discussion, without a known reverse implication. Finally, some theorems already have suitable statements and require no reformulation. Equivalence is always relative to established background mathematics. A short reduction can use a substantial representation theorem. We identify these inputs rather than include their cost in the word *elementary*.

For open problems, these statements are proposals for a future audit, as well as ways of isolating the content of the conjecture. We do not give new proofs of the underlying deep results. The contribution is the selection of statements, their precise elementary forms, and the connections between them. The arguments below are mathematical reductions; they have not been checked in a proof assistant.

Prior work and challenge theorems

Validation by consequences has a substantial history in formal methods. Rushby [57, §2.3.2] proposes *formal challenges*: putative theorems that should follow if a specification expresses its intended meaning. Madlener, Smetzers, and van Eekelen [41] use the term *challenge theorems* in a published validation of a storm-surge barrier’s control system. A challenge may test a single expected property. The term requires neither broad coverage of the specification nor a mathematically elementary statement.

Linchpins adapt this practice to the audit of substantial mathematics, with particular emphasis on the simplicity of the statement and the amount of mathematical content retained. These are additional aims, not a disjoint classification of statements. The single-curve Sato–Tate statement in §3 and the filling inequality in §8 are close to challenge theorems: each tests a restricted part of its source. The family version in §3, however, recovers the full non-CM Sato–Tate theorem over $\mathbb{Q}$. Allowing all ambient dimensions in the filling inequality still tests only a particular application of Almgren regularity.

A close precedent within formalized mathematics is Topaz’s account of the Liquid Tensor Experiment [64]. Proved examples and characterizations make its definitions accessible for inspection and guard against unintended trivializations. More recently, implication probes have been proposed for evaluating autoformalizations [43]. Our contribution is the selection and analysis of mathematical statements for this purpose, with explicit bridges and limits on what each statement audits. We make no claim to originate validation by consequences.

Guide to the examples

The source theorem and the strength retained by each proposed linchpin are listed below. The Almgren example is deliberately included as a provisional choice: it illustrates the distinction between a documented dependency and a convincing audit of a theorem’s full strength.

Source	Linchpin	Connection
Kepler conjecture	Integer points in a box, §2	Equivalent to the HOL Light statement
Sato–Tate	Cubic congruences and Catalan moments, §3	Equivalent for the specified curves
Riemann hypothesis	Three arithmetic criteria, §4	Each equivalent; open
Fundamental lemma	Twelve-square counts at primes, §5	Downstream from the unitary case
Finite simple groups	Six assignable entries; prime-power rearrangements, §6	Two classification consequences
Complex simple Lie algebras	A commutator-closed space of skew matrices, §7	Downstream through Borel’s theorem
Almgren regularity	A sharp polyhedral filling inequality, §8	Downstream; provisional as an audit
Poincaré conjecture	A polynomial with two critical points, §9	Equivalent in dimension three
Weil conjectures	Hypersurface counts; Ramanujan’s τ , §10	Equivalent to the RH part; downstream
Birch–Swinnerton-Dyer	Point-count products; rational triangles, §11	Stronger than rank BSD; conditional consequence
$P \neq NP$	Polynomial local updates on a line, §12	Equivalent; open
Boolean Pythagorean triples; $S(5) = 160$	Finite coloring statements, §13	Original statements, already elementary

Conventions

We write $\mathbb{N} = \{0, 1, 2, \dots\}$, $[n] = \{1, \dots, n\}$, and $\#S$ for the cardinality of a finite set. On $\mathbb{N}$, put

$$a \dot{-} b = \max(a - b, 0), \quad \text{adiff}(a, b) = (a \dot{-} b) + (b \dot{-} a).$$

Thus $\text{adiff}(a, b) = |a - b|$, without leaving the natural numbers. Ranks of rational or integer matrices are taken over $\mathbb{Q}$, unless another field is indicated. Limits over primes use all primes outside the finite exceptional set that is specified.

Finite lists, integer matrices, and rational numbers can be encoded by natural numbers. We usually leave these encodings implicit. Positive denominators may be cleared in a finite rational inequality. Neither convention removes an unbounded quantifier or supplies a rate of convergence.

2 The Kepler conjecture

For $x, y \in \mathbb{N}^3$, define

$$d(x, y) = \sum_{i=1}^3 \text{adiff}(x_i, y_i)^2.$$

Here d is the squared Euclidean distance.

Statement 2.1 (Integer packings in a box). *For all integers $m \geq 1$ and $n \geq 0$, and every set $S \subseteq \{0, \dots, mn\}^3$, if*

$$x, y \in S, \quad d(x, y) < 4m^2 \quad \implies \quad x = y,$$

then

$$32(\#S)^2 \leq (n + 2)^6. \tag{2.1}$$

Status. A theorem, equivalent to the proposition `the_kepler_conjecture` in the HOL Light formalization [32, §3].

The normalization is that of spheres of radius one. Dividing coordinates by m gives centers separated by at least 2, which explains the factor $4m^2$. Put

$$\rho = \frac{1}{4\sqrt{2}}, \quad \alpha = \frac{4\pi}{3}\rho = \frac{\pi}{\sqrt{18}}.$$

The number ρ is the optimal number of centers per unit volume. The HOL Light proposition, written in mathematical notation, is

$$\forall V \subseteq \mathbb{R}^3, \quad \text{packing}(V) \implies \exists c \in \mathbb{R} \forall r \geq 1, \quad \#(V \cap B(0, r)) \leq \alpha r^3 + cr^2, \quad (2.2)$$

where distinct points of a packing have distance at least 2. The constant c is allowed to depend on V .

Proposition 2.2. *Statements (2.1) and (2.2) are equivalent.*

Proof. Assume (2.2), and set $P = S/m$. The periodic set

$$W = P + (n+2)\mathbb{Z}^3$$

is a packing. Points in different copies are separated by at least 2 in some coordinate. A fundamental cube has volume $(n+2)^3$ and contains $\#S$ centers. Counting fundamental cubes that meet the boundary of a large ball gives

$$\lim_{r \rightarrow \infty} \frac{\#(W \cap B(0, r))}{(4\pi/3)r^3} = \frac{\#S}{(n+2)^3}.$$

Apply (2.2) and let r tend to infinity. This gives $\#S \leq \rho(n+2)^3$, and hence (2.1).

For the reverse implication, first consider a packing with cubic period $T > 0$ and q centers in a half-open fundamental cube. A block of k^3 cubes contains qk^3 centers. Choose an integer n_k with $kT < n_k \leq kT + 1$. Dilate this finite configuration slightly, translate it into the interior of $[0, n_k]^3$, and approximate the coordinates by rational numbers. The dilation gives strict separation greater than 2, so a sufficiently close approximation preserves separation and cardinality. Clearing a common denominator and applying (2.1) gives

$$qk^3 \leq \rho(n_k + 2)^3 \leq \rho(kT + 3)^3.$$

After division by k^3 and passage to the limit,

$$q/T^3 \leq \rho. \quad (2.3)$$

It remains to recover the quadratic boundary error in (2.2). Let $F \subset B(0, r)$ be a finite packing, with $N = \#F$. The face-centered cubic lattice

$$\Lambda = \sqrt{2}\{z \in \mathbb{Z}^3 : z_1 + z_2 + z_3 \text{ is even}\}$$

has minimum distance 2, covolume $4\sqrt{2}$, and cubic periods $T = 2\sqrt{2}k$. Choose such a period with $T > 2(r+2)$. For each translate $\Lambda + t$, delete its points in $B(Tz, r+2)$, for every $z \in \mathbb{Z}^3$, and insert $F + Tz$. The result is a periodic packing. If

$$M(t) = \#((\Lambda + t) \cap B(0, r+2)),$$

its number of centers per period is $\rho T^3 - M(t) + N$. By (2.3), $N \leq M(t)$.

Averaging t over a fundamental cube gives

$$N \leq \rho \operatorname{vol} B(0, r+2) = \alpha(r+2)^3.$$

Indeed, the average number of points of a translated lattice in a bounded measurable set is its volume divided by the lattice covolume; this follows by integrating the sum of the indicator functions of its lattice translates. A packing has finitely many centers in any bounded ball, so the estimate applies to $F = V \cap B(0, r)$. For $r \geq 1$,

$$(r+2)^3 \leq r^3 + 26r^2.$$

This proves (2.2), even with $c = 26\alpha$ independent of V . □

The shift by 2 avoids an unspecified boundary constant. An equivalent alternative is

$$\exists C \in \mathbb{N} \forall m, n \geq 1 \forall S, \quad 32(\#S)^2 \leq n^6 + Cn^5$$

under the same packing hypotheses. Statement 2.1 gives $C = 728$, by expanding $(n+2)^6$. Conversely, this alternative gives (2.3) by the same block argument.

The exponent 5 cannot be replaced by 4. For $k \geq 1$, set $n = \lceil \sqrt{2}k \rceil$, and choose $\sqrt{2} < a < n/k$ rational. The centers

$$a(i, j, \ell), \quad 0 \leq i, j, \ell \leq k, \quad i + j + \ell \text{ even},$$

form a packing in $[0, n]^3$, with

$$N \geq \frac{(k+1)^3}{2} > \rho(n + \sqrt{2} - 1)^3.$$

Thus $N^2 - n^6/32$ is bounded below by a positive constant times n^5 . Clearing denominators gives integer examples. Both the separation threshold and the boundary exponent matter.

3 Sato–Tate from cubic congruences

Let $C_j = \frac{1}{j+1} \binom{2j}{j}$ be the Catalan numbers. They can also be defined by $C_0 = 1$ and $C_{j+1} = \sum_{i=0}^j C_i C_{j-i}$. For each prime $p \neq 2, 31$, put

$$A_p = \#\{(x, y) \in \{0, \dots, p-1\}^2 : y^2 \equiv x^3 + x + 1 \pmod{p}\}, \quad h_p = \min\{h \in \mathbb{N} : h^2 \geq p\},$$

and $b_p = (p + 2h_p) \dot{-} A_p$. Write $\mathcal{P}_X = \{p \leq X : p \text{ prime}, p \neq 2, 31\}$.

Statement 3.1 (Catalan moments of cubic counts). *For every $k \in \mathbb{N}$,*

$$\lim_{X \rightarrow \infty} \frac{1}{\#\mathcal{P}_X} \sum_{p \in \mathcal{P}_X} \left(\frac{b_p}{h_p} \right)^k = C_{k+1}. \quad (3.1)$$

Status. A theorem, equivalent to Sato–Tate for $y^2 = x^3 + x + 1$. The nonintegral- j theorem of Harris–Shepherd–Barron–Taylor suffices [33].

This statement tests one curve. It does not by itself recover the theorem for all non-CM elliptic curves; the family version below does.

The curve has discriminant $-16 \cdot 31$ and $j = 6912/31$. It has no complex multiplication, since a rational complex-multiplication j -invariant is an integer [61]. The affine count A_p omits one point at infinity. Consequently the Frobenius trace is $a_p = p - A_p$. Hasse's bound $|a_p| \leq 2\sqrt{p}$ [60] shows that the truncated subtraction loses nothing and that

$$z_p := b_p/h_p = 2 + a_p/h_p \in [0, 4], \quad |z_p - (2 + a_p/\sqrt{p})| \leq 2/h_p \longrightarrow 0.$$

Sato–Tate says that $a_p/(2\sqrt{p})$ has limiting density $(2/\pi)\sqrt{1-t^2}$ on $[-1, 1]$. After the change of variable $z = 2 + 2t$, the density is

$$d\nu(z) = \frac{1}{2\pi} \sqrt{z(4-z)} dz, \quad 0 \leq z \leq 4.$$

A beta integral gives

$$\int_0^4 z^k d\nu(z) = \frac{1}{k+2} \binom{2k+2}{k+1} = C_{k+1}. \quad (3.2)$$

Thus Sato–Tate implies (3.1). Conversely, convergence of these moments gives convergence against every polynomial. Polynomial approximation on $[0, 4]$ gives convergence against every continuous function. The vanishing rounding error then recovers Sato–Tate. This is the full distribution statement for the curve, including the signs of its traces.

For an entirely arithmetic version, let $X \geq 3$, $D_X = X!$, $G_X = \#\mathcal{P}_X$, and

$$U_{k,X} = \sum_{p \in \mathcal{P}_X} (b_p(D_X/h_p))^k.$$

The divisions are exact. Statement 3.1 is equivalent to

$$\begin{aligned} \forall k \geq 0 \ \forall q \geq 1 \ \exists X_0 \geq 3 \ \forall X \geq X_0, \\ q \text{ adiff}(U_{k,X}, C_{k+1} G_X D_X^k) \leq G_X D_X^k. \end{aligned} \quad (3.3)$$

In this form there are no real numbers in the statement.

The same construction applies to

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}, \quad D = 4A^3 + 27B^2 \neq 0,$$

using primes $p \nmid 2D$. The elementary condition $D \nmid 6912A^3$ says that $j = 6912A^3/D$ is not an integer. Quantifying (3.1) over this family is equivalent to the nonintegral- j case of Sato–Tate over $\mathbb{Q}$.

One can cover every non-CM elliptic curve over $\mathbb{Q}$ by excluding the following fixed set:

$$\begin{aligned} J = \{0, 12^3, -15^3, 20^3, -32^3, 2 \cdot 30^3, 66^3, \\ -96^3, -3 \cdot 160^3, 255^3, -960^3, -5280^3, -640320^3\}. \end{aligned}$$

These are the rational CM j -invariants, from the classical class-number-one classification [20]. Replace the nonintegrality condition by

$$6912A^3 \neq cD \quad \text{for every } c \in J.$$

Every elliptic curve over $\mathbb{Q}$ admits an integral short Weierstrass equation. Changes of model affect only finitely many excluded primes. The resulting family of moment assertions is therefore equivalent to the full non-CM Sato–Tate theorem over $\mathbb{Q}$ [6, Corollary 8.9]. This last equivalence uses the classification of rational CM invariants in addition to the elementary moment argument.

4 Three formulations of the Riemann hypothesis

The following three statements retain different features of the Riemann hypothesis. The first has the shortest notation. The second asks for finite certificates of approximation. The third consists entirely of universal rational inequalities.

4.1 Squarefree counting

Let $E(n)$ and $O(n)$ count the squarefree integers in $[n]$ with, respectively, an even and an odd number of distinct prime factors. The integer 1 is counted in $E(n)$. Put $D(n) = \text{adiff}(E(n), O(n))$.

Statement 4.1 (Squarefree cancellation). *For every integer $k \geq 1$, there is $N \geq 1$ such that*

$$D(n)^{2k} \leq n^{k+1} \quad (n \geq N).$$

Status. Open; equivalent to the Riemann hypothesis.

Let $M(x) = \sum_{a \leq x} \mu(a)$, where μ is the Möbius function. Then $D(n) = |M(n)|$. Littlewood's criterion states

$$\text{RH} \iff M(x) = O_\varepsilon(x^{1/2+\varepsilon}) \quad \text{for every } \varepsilon > 0;$$

see [40, 63]. Under RH use $\varepsilon = 1/(4k)$ and absorb the constant into $n^{1/2}$ after raising to the power $2k$. Conversely, choose k arbitrarily large.

The direction from cancellation to RH has a short explanation. Partial summation makes

$$s \int_1^\infty M(x) x^{-s-1} dx$$

holomorphic on $\Re s > 1/2$. It agrees with $1/\zeta(s)$ on $\Re s > 1$, so the zeta function has no zeros to the right of the critical line. Its functional equation gives the remaining assertion. The reverse implication is the substantial analytic part of the criterion.

4.2 Approximation by remainders

Write $r_d(n)$ for the remainder on dividing n by d . For $m \geq 2$ and $c_2, \dots, c_m \in \mathbb{Q}$, put

$$F_c(n) = \sum_{d=2}^m c_d r_d(n), \quad B_c = 1 + \sum_{d=2}^m |c_d|(d-1).$$

Statement 4.2 (Finite remainder certificates). *For every integer $q \geq 1$, there are integers $m \geq 2$, $N \geq 1$ and rational numbers $c_2, \dots, c_m$ such that*

$$q \left(\sum_{n=1}^N \frac{(1 - F_c(n))^2}{n(n+1)} + \frac{B_c^2}{N+1} \right) < 1. \quad (4.1)$$

Status. Open; equivalent to RH by the Nyman–Beurling–Báez-Duarte criterion, in its sequence form.

The sequence criterion says that RH is equivalent to the constant sequence 1 belonging to the closed linear span of the remainder sequences in the norm

$$\|f\|^2 = \sum_{n=1}^\infty \frac{|f(n)|^2}{n(n+1)}.$$

Bagchi gives this precise sequence version [5, Theorem 1], using the fractional parts $r_d(n)/d$, which have the same linear span. Its analytic antecedents are [48, 7, 4]. Real coefficients suffice by taking real parts, and rational coefficients suffice by finite-dimensional approximation.

Since $|1 - F_c(n)| \leq B_c$, the omitted tail has the explicit bound

$$\sum_{n>N} \frac{(1 - F_c(n))^2}{n(n+1)} \leq B_c^2 \sum_{n>N} \left(\frac{1}{n} - \frac{1}{n+1} \right) = \frac{B_c^2}{N+1}.$$

This proves one implication. For the other, first choose an approximation with squared norm less than $1/(2q)$, then make $B_c^2/(N+1) < 1/(2q)$. Every witness to (4.1) is checked by a finite rational calculation.

Borisov's work connects this circle of ideas with factorial ratios and quotient singularities [12]. It provides a relevant geometric context, but the remainder criterion above is attributed to the Nyman–Beurling–Báez-Duarte theory.

4.3 A rational form of Lagarias's inequality

Set

$$H_n = \sum_{j=1}^n \frac{1}{j}, \quad \sigma(n) = \sum_{d|n} d.$$

For rational $h \geq 1$ and integer $m > h$, define

$$U_m(h) = \left(\frac{m}{m-h} \right)^m, \quad V_m(h) = (h-1) \sum_{j=0}^{m-1} \frac{1}{m+j(h-1)}.$$

Statement 4.3 (Divisor sums and rational upper bounds). *For every $n \geq 1$ and every $m \geq n+1$,*

$$\sigma(n) \leq H_n + U_m(H_n)V_m(H_n). \quad (4.2)$$

Status. Open; equivalent to RH by Lagarias's theorem [38], which uses Robin's work [56].

Lagarias's criterion is

$$\sigma(n) \leq H_n + e^{H_n} \log H_n \quad (n \geq 1). \quad (4.3)$$

For fixed $h \geq 1$, the exponential limit gives $U_m(h) \geq e^h$ and $U_m(h) \rightarrow e^h$. The quantity $V_m(h)$ is the left Riemann sum for $\int_1^h dt/t$, so $V_m(h) \geq \log h$ and $V_m(h) \rightarrow \log h$. These quantities are nonnegative. Thus (4.3) implies (4.2); letting $m \rightarrow \infty$ proves the converse. All denominators are positive because $H_n \leq n < m$.

Clearing denominators makes Statement 4.3 a universal assertion about natural numbers. For example, $H_n = A_n/n!$, where $A_n = \sum_{j=1}^n n!/j$ is an integer. If RH is false, a finite pair (n, m) violates (4.2), and the violation is verifiable by exact arithmetic. This is a statement about the form of a possible counterexample, not a method for finding one.

5 The fundamental lemma and twelve squares

Define

$$R_{12}(n) = \#\{(x_1, \dots, x_{12}) \in \mathbb{Z}^{12} : x_1^2 + \dots + x_{12}^2 = n\}.$$

Order and signs are counted. For an odd prime p , put

$$h_p = \min\{h \in \mathbb{N} : h^2 \geq p^5\}, \quad b_p = (R_{12}(p) + 32h_p) \dot{-} 8(p^5 + 1),$$

and $P(X) = \#\{p \leq X : p \text{ is an odd prime}\}.$

Statement 5.1 (Moments of twelve-square counts). *For every $k \in \mathbb{N}$,*

$$\lim_{X \rightarrow \infty} \frac{1}{P(X)} \sum_{\substack{3 \leq p \leq X \\ p \text{ prime}}} \left(\frac{b_p}{16h_p} \right)^k = C_{k+1}.$$

Status. A theorem, equivalent to the twelve-square distribution theorem of Barnet-Lamb–Geraghty–Harris–Taylor [6, Corollary 8.6]. Their proof is downstream from the fundamental lemma for unitary groups. No equivalence with the fundamental lemma is asserted.

The connection was noted in Hales’s account of Ngô’s work [31, Theorem 2]. For odd primes,

$$R_{12}(p) = 8(p^5 + 1) + 16a_p, \quad \sum_{n \geq 1} a_n q^n = q \prod_{j \geq 1} (1 - q^{2j})^{12}. \quad (5.1)$$

The product is a modular form of weight 6 and level 4. Its normalized coefficients $a_p/(2p^{5/2})$ have the semicircle distribution on $[-1, 1]$. Deligne’s coefficient bound $|a_p| \leq 2p^{5/2}$ [23, Theorem 8.2] shows that the subtraction in b_p does not truncate. Moreover,

$$0 \leq \frac{b_p}{16h_p} \leq 4, \quad \frac{b_p}{16h_p} - \left(2 + \frac{a_p}{p^{5/2}} \right) \rightarrow 0.$$

The argument of §3, including (3.2), proves the asserted equivalence. Deligne’s bound supplies the common compact interval needed to pass between moments and distributions; it is an additional established dependency of this bridge.

The dependency on the fundamental lemma can be identified more precisely than a general appeal to the Langlands program. The construction of automorphic Galois representations used in [6, §1] invokes the unitary-group fundamental lemma of Laumon–Ngô [39], together with transfer results of Waldspurger [67]. These representations enter the potential automorphy argument that proves the distribution theorem. Thus this example tests a substantial case of the fundamental lemma, already available before Ngô’s general theorem [47]. It should not be described as requiring the full generality of that later result.

An especially short consequence retains only the sign of the error. Let

$$A(X) = \#\{p \leq X : p \text{ odd prime, } R_{12}(p) > 8(p^5 + 1)\}.$$

Then

$$\forall q \geq 1 \exists X_0 \geq 3 \forall X \geq X_0, \quad q \operatorname{adiff}(2A(X), P(X)) \leq P(X). \quad (5.2)$$

The positive and negative halves of the semicircle each have measure 1/2. Statement (5.2) is therefore downstream from Statement 5.1, but it loses most of the distribution theorem.

The integer count itself can be written using only natural numbers:

$$R_{12}(n) = \sum_{\substack{x_1, \dots, x_{12} \in \{0, \dots, n\} \\ x_1^2 + \dots + x_{12}^2 = n}} 2^{\#\{i: x_i > 0\}}.$$

Replacing a limit by its quantified definition and clearing the finite denominators gives an arithmetic statement, as in (3.3). No modular forms or Galois representations occur in the resulting statement.

6 Consequences of the classification of finite simple groups

A list $a = (a_0, \dots, a_{n-1})$ will be called a *rearrangement* if its entries are precisely $0, \dots, n-1$, each occurring once. For two rearrangements define

$$a * b = (a_{b_0}, \dots, a_{b_{n-1}}).$$

A nonempty set of rearrangements closed under this operation is a permutation group: powers of any element give the identity and its inverse. The following statements avoid group-theoretic terminology in their hypotheses and conclusions.

Statement 6.1 (Six freely assignable entries). *Let $n \geq 6$, and let S be a set of rearrangements of $0, \dots, n-1$. Suppose that $a * b \in S$ whenever $a, b \in S$. Suppose also that, for every six pairwise distinct numbers $y_0, \dots, y_5 < n$, some $a \in S$ satisfies $a_i = y_i$ for $0 \leq i \leq 5$. Then*

$$2\#S \geq n!.$$

Status. A theorem downstream from the classification of finite simple groups (CFSG). It is equivalent to the classification consequence that every finite 6-transitive permutation group is alternating or symmetric.

The six-entry condition means that the orbit of the ordered tuple $(0, 1, \dots, 5)$ contains every ordered tuple of distinct entries. For a group this is exactly 6-transitivity. The classification of multiply transitive permutation groups gives $S = A_n$ or S_n ; see [15, 3]. Conversely, the displayed bound gives $[S_n : S] \leq 2$. The only subgroup of index two in S_n is A_n . Thus the translation loses no content of this consequence of CFSG.

The factor 2 is attained by A_n for $n \geq 8$. The number six cannot be replaced by five: the Mathieu group M_{12} , of order 95040, is sharply 5-transitive and has order less than $12!/2$. These facts are part of the standard permutation-group description [15].

For a rearrangement a , define $a^{[0]}(i) = i$ and $a^{[r+1]}(i) = a_{a^{[r]}(i)}$.

Statement 6.2 (A prime-power rearrangement). *Let $n > 1$, and let S be a composition-closed set of rearrangements such that, for every $y < n$, some $a \in S$ has $a_0 = y$. Then there are $a \in S$, a prime p , and an integer $k \geq 1$, with $p^k \leq n$, such that*

$$a_i \neq i \quad \text{and} \quad a^{[p^k]}(i) = i \quad (0 \leq i < n).$$

Status. A theorem downstream from CFSG, equivalent to the Fein–Kantor–Schacher theorem [26].

The latter theorem states that a finite transitive permutation group of degree greater than one has a fixed-point-free element of prime-power order. For a permutation of prime-power order, the order equals the length of its longest cycle, and is at most n . Conversely, the displayed conditions imply that the order of a is a nontrivial power of p . The original proof of Fein–Kantor–Schacher explicitly invokes the classification. Neither of these two linchpins is asserted to imply CFSG.

7 Cartan’s classification and a row of a matrix

The source here is the Killing–Cartan classification of finite-dimensional nonabelian simple Lie algebras over $\mathbb{C}$, up to isomorphism: the four classical families and five exceptional types. The form used most directly by Borel is the corresponding classification of compact real simple Lie algebras. Complexification and passage to the compact real form give inverse correspondences between these

isomorphism classes; the compact real form exists and is unique up to isomorphism [36, 37]. The classification of all real forms is not needed here.

The following statement starts with an arbitrary commutator-closed space of matrices. Thus the structural theory of Lie algebras enters before any classification of root systems can be applied.

Statement 7.1 (One unrestricted row). *Let $n \geq 9$ be odd. Let V be a $\mathbb{Q}$ -linear subspace of the skew-symmetric $n \times n$ rational matrices. Suppose that*

$$A, B \in V \implies AB - BA \in V$$

and that every vector of $\mathbb{Q}^{n-1}$ occurs as the last $n-1$ entries of the first row of a matrix in V . Then

$$V = \{A \in M_n(\mathbb{Q}) : A^\top = -A\}.$$

Status. A theorem downstream from the classification of complex simple Lie algebras, through their compact real forms and Borel's classification of compact connected groups transitive on even-dimensional spheres [11]. No converse to Cartan's classification is claimed.

Borel's theorem says that the Lie algebra of an effective compact connected group transitive on S^{2r} is $\mathfrak{so}(2r+1)$, except that $\mathfrak{g}_2$ is also possible on S^6 . There are two steps in his argument. Theorem II shows that the group is simple, using the simple connectivity of the sphere and its Euler characteristic 2. Theorem III then classifies the possible simple groups, explicitly using the Killing–Cartan classification [11, pp. 583–586, Theorems II and III].

Here is the reduction. Extend scalars to $\mathfrak{h} = \text{span}_{\mathbb{R}} V \subseteq \mathfrak{so}(n)$, and let G be the closure in $\text{SO}(n)$ of the subgroup generated by $\exp(\mathfrak{h})$. It is compact and connected. At e_1 , the possible tangent vectors include

$$\{Xe_1 : X \in \mathfrak{h}\} = e_1^\perp.$$

Hence the orbit of e_1 is open in S^{n-1} . It is closed by compactness, so it is the whole sphere. Borel's theorem gives $G = \text{SO}(n)$. Here $n-1$ is even. The bound $n \geq 9$ is chosen for convenience to exclude the exceptional G_2 action on S^6 .

One must still account for the passage to the closure. The space $\mathfrak{h}$ is invariant under conjugation by each $\exp(X)$ with $X \in \mathfrak{h}$. It is therefore invariant under G . Consequently it is a nonzero ideal of $\mathfrak{so}(n)$. This algebra is simple for $n \geq 5$, so $\mathfrak{h} = \mathfrak{so}(n)$. Equality of dimensions gives the result over $\mathbb{Q}$.

There is a finite integer version. Given skew-symmetric integer matrices $A_1, \dots, A_s$, let $u(A)$ list the entries above the diagonal, and set

$$C = [u(A_1) \ \cdots \ u(A_s)].$$

Let R be the submatrix in the rows indexed by $(1, 2), \dots, (1, n)$. For odd $n \geq 9$, the assertion is

$$\left. \begin{array}{l} \text{rank } R = n-1, \\ \text{rank}[C \ u(A_i A_j - A_j A_i)] = \text{rank } C \quad (1 \leq i, j \leq s) \end{array} \right\} \implies \text{rank } C = \frac{n(n-1)}{2}. \quad (7.1)$$

Every condition is a condition on integer minors. Conversely, a rational subspace has a basis that becomes integral on clearing denominators, so this version is equivalent to Statement 7.1.

The dimension restrictions are genuine. When $n = 2m$, matrices

$$\begin{pmatrix} P & -Q \\ Q & P \end{pmatrix}, \quad P^\top = -P, \quad Q^\top = Q,$$

give a proper commutator-closed rational space with an unrestricted first row, for $m \geq 2$. Its dimension is m^2 . In dimension seven, the compact algebra $\mathfrak{g}_2$ in its octonionic representation gives the exceptional transitive action. These are structural obstructions to the conclusion, rather than features of a chosen root diagram.

8 Almgren regularity and polyhedral fillings

Almgren's regularity theorem bounds the Hausdorff dimension of the interior singular set of an m -dimensional area-minimizing integral current by $m - 2$ [1]. A current may be regarded, for the present purpose, as a generalized oriented surface with integer multiplicity, for which volume and boundary remain defined under limits. The linchpin below avoids this language in its statement.

Fix an ambient dimension $N \geq 3$. A rational polyhedral k -chain in $\mathbb{R}^N$ is a finite integer linear combination of oriented affine k -simplices with rational vertices, taken modulo subdivision and cancellation. Its boundary is the alternating sum of its faces, extended linearly. For $x = (x_1, \dots, x_N)$, set

$$G(x) = \text{diag}(1, 1 + x_1^2, \dots, 1 + x_N^2).$$

If $\sigma = [v_0, \dots, v_k]$, write $B = (v_1 - v_0, \dots, v_k - v_0)$ and $\Delta_k = \{u \in \mathbb{R}^k : u_i \geq 0, \sum u_i \leq 1\}$. Define

$$W_k(\sigma) = \int_{\Delta_k} \sqrt{\det(B^\top G(v_0 + Bu)B)} du. \quad (8.1)$$

For a chain, subdivide to account for overlaps, cancel opposite multiplicities, and sum with absolute multiplicities.

Statement 8.1 (A sharp weighted filling inequality). *For every $N \geq 3$, every rational polyhedral 2-chain P in $\mathbb{R}^N$ with $\partial P = 0$, and every integer $r \geq 1$, there is a rational polyhedral 3-chain Q in $\mathbb{R}^N$ such that*

$$\partial Q = P, \quad 36\pi W_3(Q)^2 < W_2(P)^3 + \frac{1}{r}.$$

Status. A theorem downstream from Almgren regularity through Schulze's sharp isoperimetric inequality [59]. As a linchpin for Almgren's theorem it is provisional: the proof dependency is documented, but the possibility of a bypass is substantial.

Formula (8.1) is the simplex volume for the metric

$$g = dt^2 + (1 + t^2)(dy_1^2 + \dots + dy_{N-1}^2) \quad \text{on } \mathbb{R}^N.$$

The metric dominates the Euclidean metric and is complete. Its underlying space is simply connected. With $f(t) = \sqrt{1 + t^2}$, the mixed and horizontal sectional curvatures are, respectively,

$$-f''/f = -\frac{1}{(1 + t^2)^2}, \quad -(f'/f)^2 = -\frac{t^2}{(1 + t^2)^2}.$$

The warped-product curvature formula therefore gives nonpositive sectional curvature [49].

Schulze's theorem applies in every ambient dimension $N \geq 3$, in a complete simply connected manifold of nonpositive sectional curvature. A compact integral 2-cycle P in our space has a compact least-mass integral 3-dimensional filling T . Indeed, coning gives a compact competitor. Nearest-point projection onto a closed geodesic ball containing P fixes P and does not increase mass [14, Proposition II.2.4]. The ball is compact by completeness, so integral-current compactness and lower semicontinuity give a minimizer [25, §§4.2.16–4.2.17]. Schulze's inequality is

$$36\pi \mathbf{M}_g(T)^2 \leq \mathbf{M}_g(P)^3 \quad [59, \text{Theorem 1.2}].$$

The indices 2 and 3 are the dimensions of the boundary and the filling. The constant 36π comes from the area and volume of an ordinary Euclidean three-ball: $36\pi(4\pi/3)^2 = (4\pi)^3$. It is independent of N . In particular, ambient dimension six has no special role in the inequality. Changing the

dimensions of the boundary and filling would be a different generalization, with different exponents and constant. Schulze's sharp theorem does not give that generalization; his Remark 1.5 discusses non-sharp estimates in other dimensions.

The passage to rational chains requires an approximation relative to the prescribed boundary. We give the details, including the change from Euclidean to Riemannian mass.

Lemma 8.2 (Relative rational approximation). *Let g be a smooth Riemannian metric on $\mathbb{R}^N$, and let T be a compactly supported integral k -current, $1 \leq k \leq N$. Suppose that $\partial T = P$ is a rational polyhedral chain. For every $\varepsilon > 0$, there is a rational polyhedral chain Q with integer coefficients such that*

$$\partial Q = P, \quad \mathbf{M}_g(Q) < \mathbf{M}_g(T) + \varepsilon.$$

Proof. Write $\mathbf{M}$ for Euclidean mass. We first obtain polyhedral chains with real vertices, integer coefficients, the exact boundary P , and convergent Euclidean mass. Integral polyhedral approximation [25, §§4.2.21–4.2.22] gives chains B_j with $\mathbf{M}(B_j) \rightarrow \mathbf{M}(T)$ and decompositions

$$T - B_j = U_j + \partial V_j, \quad \mathbf{M}(U_j) + \mathbf{M}(V_j) \rightarrow 0,$$

where U_j, V_j are integral currents and all supports lie in a fixed compact set. This is approximation in the integral flat norm, so the correction currents also have integer multiplicities. Since $\partial U_j = P - \partial B_j$ is polyhedral, the integral deformation theorem [25, §4.2.9], with mesh δ_j , gives

$$U_j = R_j + E_j + \partial Z_j,$$

where R_j, E_j are integral polyhedral chains and

$$\begin{aligned} \mathbf{M}(R_j) &\leq C(\mathbf{M}(U_j) + \delta_j \mathbf{M}(\partial U_j)), \\ \mathbf{M}(E_j) &\leq C\delta_j \mathbf{M}(\partial U_j), \quad \mathbf{M}(Z_j) \leq C\delta_j \mathbf{M}(U_j). \end{aligned}$$

Here C depends only on the dimensions. The fact that the boundary is polyhedral makes the boundary error E_j polyhedral as well; see also the two-step argument in [16, §1.2]. Choose $\delta_j \rightarrow 0$ with $\delta_j \mathbf{M}(\partial U_j) \rightarrow 0$, and set $A_j = B_j + R_j + E_j$. Then

$$\partial A_j = P, \quad T - A_j = \partial(V_j + Z_j).$$

Thus $A_j \rightarrow T$ in flat norm and $\limsup \mathbf{M}(A_j) \leq \mathbf{M}(T)$; lower semicontinuity gives $\mathbf{M}(A_j) \rightarrow \mathbf{M}(T)$. The deformation moves supports by at most a constant times δ_j , so a common compact set still contains them.

Regard these currents as measures with values in the Euclidean space $\Lambda^k \mathbb{R}^N$. Flat convergence and the uniform mass bound give weak convergence of these vector measures. Because the currents are rectifiable, their polar vectors are simple, and their Euclidean total variations are exactly their masses. The convergence just proved therefore satisfies the hypotheses of Reshetnyak's continuity theorem [55]; see [2, Theorem 2.39]. Apply it to the continuous function $\Phi_g(x, \xi) = |\xi|_{g_x}$, the norm on exterior powers induced by the metric, restricted to Euclidean unit vectors ξ . On a common compact neighborhood this function is bounded. We obtain

$$\mathbf{M}_g(A_j) \rightarrow \mathbf{M}_g(T).$$

Fix $A = A_j$ with $\mathbf{M}_g(A) < \mathbf{M}_g(T) + \varepsilon/2$.

It remains to make the vertices rational without changing the boundary chain. Represent P on a finite rational simplicial complex L , and choose a common finite triangulation K of A and L . The

subdivision may introduce irrational vertices on L , so simply fixing all boundary vertices would not suffice. For each vertex of K on $|L|$, choose a nearby rational point in the smallest face of L containing it. Such points are dense in that face. Choose nearby rational points for the remaining vertices, and extend these choices affinely over each simplex of K , obtaining a piecewise affine map f .

For every subdivided simplex of P , both f and the straight homotopy $H(s, x) = (1 - s)x + sf(x)$ remain in the same face of L , of dimension at most $k - 1$. Hence the swept-out k -current $H_{\#}([0, 1] \times P)$ is zero. Since $\partial P = 0$, the homotopy formula gives

$$f_{\#}P - P = \partial H_{\#}([0, 1] \times P) = 0.$$

Consequently $Q = f_{\#}A$ is rational polyhedral with integer coefficients and $\partial Q = f_{\#}P = P$. Write $A = \sum_{\sigma} a_{\sigma} \sigma$ on K , after cancellation. The g -volume of each of these finitely many simplices is continuous in its vertices. Thus the choices can be made so close that

$$\mathbf{M}_g(Q) \leq \sum_{\sigma} |a_{\sigma}| \mathbf{M}_g(f_{\#}\sigma) < \mathbf{M}_g(A) + \varepsilon/2.$$

Possible overlaps in the images only decrease mass after cancellation. This proves the lemma. $\square$

Apply the lemma to the minimizing filling T , choosing $\varepsilon > 0$ so small that

$$36\pi((\mathbf{M}_g(T) + \varepsilon)^2 - \mathbf{M}_g(T)^2) < 1/r.$$

For polyhedral chains the metric mass is exactly the weighted volume in (8.1). Schulze's inequality and $\partial Q = P$ now give Statement 8.1.

Schulze invokes Almgren's singular-set bound for minimizing *three*-currents in the uniqueness argument of [59, §5, Lemma 5.2]. Here Almgren gives Hausdorff dimension at most $3 - 2 = 1$ for the interior singular set. This codimension two is measured within the three-dimensional current; the ambient codimension of the filling is $N - 3$. Varying N thus includes three-dimensional fillings in arbitrary codimension, but does not test Almgren's theorem in every intrinsic dimension. Small regular patches are removed from a minimizing filling. The codimension-two singular-set estimate and unique continuation are used to obtain uniqueness for the remaining problem, which enters the proof of the isoperimetric inequality. This is a specific use of the regularity theorem, rather than an appeal to an unspecified result of Almgren.

There are reasons for caution about the choice of linchpin. The metric has translations and rotations in the y -variables, and projection onto $t = 0$ contracts lengths. When $N \geq 4$, its sharp constant is already witnessed by Euclidean round three-balls in that slice. These facts leave room for a special proof that avoids the regularity theorem. Moreover, another uniqueness argument might replace its use in Schulze's proof.

Projection alone does not prove the result: it changes the prescribed boundary. For example, when $N \geq 4$, the cylinder needed to restore a small two-sphere at height $t_0 \neq 0$ has volume of order its radius squared, whereas the desired filling estimate has order its radius cubed. Thus the most immediate shortcut fails. Nevertheless, no converse has been established, and no claim of indispensability is justified. This example records a valid consequence and an unresolved question about its value as an audit.

The same argument gives a broader version: allow any symmetric rational-polynomial $N \times N$ matrix field G with $G(x) \succeq I$ and nonpositive sectional curvature, and use (8.1) with this G . The lower bound on the metric ensures completeness. This removes the symmetry of the particular example, but it still gives no reverse implication to Almgren regularity and no assertion that this polynomial class represents every relevant geometry.

If desired, the integrals can be removed from the formal statement. Their integrands are square roots of nonnegative rational polynomials on rational simplices. Subdivision and explicit continuity estimates give rational upper and lower bounds to arbitrary accuracy; the same is true of π . A strict inequality therefore has a finite rational certificate. The resulting assertion has the form $\forall P, r \exists Q, s$, where s certifies the numerical inequality and all checks are finite.

9 Poincaré in dimension three

Here the polynomial models cover every closed smooth three-manifold. This representation theorem prevents the loss of generality that is a concern in the preceding example.

Statement 9.1 (Two critical points on a polynomial three-manifold). *Let $p_1, \dots, p_s \in \mathbb{Z}[x_1, \dots, x_7]$, and set*

$$X = \{x \in \mathbb{R}^7 : p_1(x) = \dots = p_s(x) = 0\}.$$

Suppose that:

1. *X is nonempty, bounded, and connected;*
2. *at each point of X , four of the p_i have independent gradients, and their common zero set agrees locally with X ;*
3. *every continuous map $S^1 \rightarrow X$ extends to a continuous map of the closed disk into X .*

Then there is $h \in \mathbb{Z}[x_1, \dots, x_7]$ such that $h|_X$ has exactly two critical points, both nondegenerate.

Status. A theorem equivalent to the three-dimensional Poincaré conjecture, using smooth structures in dimension three, the rational Nash–Tognoli theorem, and elementary Morse theory. Perelman’s work proves the source theorem [50, 51, 52]; see also [45].

The first two assumptions say that X is a compact connected smooth three-manifold without boundary. The third says it is simply connected. A critical point is taken along X ; the ambient gradient of h need not vanish.

Assume Poincaré. Uniqueness of smooth structures in dimension three [44] gives a diffeomorphism $X \rightarrow S^3$. Pull back the ordinary height function on S^3 . It has two nondegenerate critical points. Extend this smooth function to an ambient neighborhood and approximate it in the C^2 norm on a compact neighborhood by a polynomial. Such approximation follows, for example, by polynomial approximation with derivatives on a box after taking a smooth extension. Rational coefficients can be used by a further sufficiently small perturbation.

A sufficiently small C^2 perturbation preserves the two Morse critical points and creates no others. Near each critical point, nondegeneracy gives stability; on the complement of small neighborhoods the tangential gradient has a positive lower bound. Multiplying the rational polynomial by a positive common denominator gives the required integer polynomial.

Conversely, a compact connected manifold with a Morse function having exactly two critical points is homeomorphic to a sphere [42, Theorem 4.1]. In dimension three, neighborhoods of the minimum and maximum are balls, and the region between them is $S^2 \times [0, 1]$. Gluing the two balls along their boundary gives S^3 , since a homeomorphism of S^2 extends over the ball.

To apply this to an arbitrary closed smooth three-manifold, use the rational Nash–Tognoli theorem of Ghiloni–Savi [28, Theorem 1.7]. Every compact smooth d -manifold has a nonsingular algebraic model in $\mathbb{R}^{2d+1}$, with both its global equations and its local nonsingularity defined over $\mathbb{Q}$. For $d = 3$ this is $\mathbb{R}^7$. A finite generating family for the rational vanishing ideal provides the

required equations; locally, four of its gradients are independent. Clear denominators. The linchpin now proves Poincaré for smooth three-manifolds, and existence of smooth structures in dimension three [44] gives the topological statement.

The conclusion also has a direct algebraic description. Let $J(x)$ have rows $\nabla p_i(x)^\top$. On X , $\text{rank } J(x) = 4$ and $T_x X = \ker J(x)$. A point is critical precisely when

$$\text{rank} \begin{pmatrix} J(x) \\ \nabla h(x)^\top \end{pmatrix} = 4.$$

Choose four local defining equations $q_1, \dots, q_4$ with independent gradients, and at a critical point write $\nabla h = \sum_i \lambda_i \nabla q_i$. Nondegeneracy means that the quadratic form

$$D^2 h - \sum_{i=1}^4 \lambda_i D^2 q_i$$

is nonsingular on $\ker J(x)$. Thus the assertion about a proposed h is expressible by real polynomial equations and inequalities. The hypothesis about loops is retained in its usual topological form. There is no imposed bound on the degree of h .

10 The Weil conjectures

We distinguish two linchpins. The first retains the Riemann-hypothesis part of the Weil conjectures, using a substantial reduction theorem. The second is the familiar Ramanujan inequality, whose statement is particularly short.

10.1 Counting zeros of a homogeneous polynomial

Let K be a finite field with q elements, and let $F \in K[x_1, \dots, x_m]$ be nonzero and homogeneous of degree $d \geq 1$, where $m \geq 3$. Impose the following smoothness condition: in every finite extension K'/K ,

$$F(x) = \frac{\partial F}{\partial x_1}(x) = \dots = \frac{\partial F}{\partial x_m}(x) = 0 \implies x = 0. \quad (10.1)$$

Including $F(x) = 0$ is necessary when the characteristic divides d . This condition says exactly that the projective hypersurface is smooth. Put $A(F, K) = \#\{x \in K^m : F(x) = 0\}$.

Statement 10.1 (A hypersurface counting inequality). *For every K, m, d, F as above satisfying (10.1),*

$$(A(F, K) - q^{m-1})^2 \leq (d-1)^{2m-2} q^m. \quad (10.2)$$

Status. A theorem. It is equivalent to the Riemann-hypothesis part of the Weil conjectures for all smooth proper varieties over finite fields, using the cohomological background and Scholl's reduction [58]. It is not presented as a reformulation of every part of the Weil conjectures at once.

Here is the connection. Let $X \subset \mathbb{P}_K^{m-1}$ be the hypersurface $F = 0$, of dimension $n = m - 2$. Then

$$A(F, K) = 1 + (q-1)\#X(K), \quad q^{m-1} = 1 + (q-1)(1 + q + \dots + q^n).$$

The trace formula and weak Lefschetz theorem express the difference $\#X(K) - (1 + \dots + q^n)$ as the signed trace on the primitive middle cohomology. Its dimension is

$$B_{m,d} = \frac{(d-1)^m + (-1)^m(d-1)}{d} \leq (d-1)^{m-1};$$

see [29, §4]. Deligne's theorem [23] bounds each eigenvalue in this cohomology by $q^{n/2}$ in absolute value. It follows that

$$|A(F, K) - q^{m-1}| \leq (q-1)B_{m,d}q^{(m-2)/2} \leq (d-1)^{m-1}q^{m/2},$$

which proves (10.2).

For the converse, fix F and apply (10.2) over every extension of degree r . Dividing by $q^r - 1$ gives

$$\left| \#X(\mathbb{F}_{q^r}) - \sum_{j=0}^n q^{rj} \right| \leq 2(d-1)^{m-1}q^{rn/2}.$$

If $\alpha_1, \dots, \alpha_B$ are the primitive middle eigenvalues, the trace formula identifies the left side with $|\sum_i \alpha_i^r|$.

We use the elementary power-sum observation that

$$\left| \sum_{i=1}^B \alpha_i^r \right| = O(R^r) \ (r \geq 1) \implies |\alpha_i| \leq R \text{ for every } i.$$

Indeed, the generating function of these sums is $\sum_i \alpha_i z / (1 - \alpha_i z)$. A nonzero eigenvalue of modulus greater than R would give a pole inside its disk of convergence. Equal eigenvalues add their positive multiplicities, so their poles cannot cancel. Apply this observation to every complex realization of the eigenvalues. Poincaré duality pairs α with q^n/α , giving $|\alpha| = q^{n/2}$. The remaining cohomology of a smooth hypersurface is the known ambient cohomology. Thus the counting inequality recovers the Riemann hypothesis for smooth hypersurfaces.

Scholl's theorem states that the Riemann hypothesis in dimension $d-1$, together with that for smooth hypersurfaces of dimension d , implies it for all smooth proper varieties of dimension d [58, Theorem 3.3]. Induction, starting in dimension zero, completes the converse. Scholl's reduction uses de Jong's alterations [21, 22], the Rapoport–Zink vanishing-cycles spectral sequence [54], and Deligne's local monodromy theorem for punctually pure sheaves on curves [24, Theorem 1.8.4]; the last is recalled as Theorem 1.9 of [58]. These are established dependencies of the reduction, not further conjectures. In particular, the local monodromy theorem used here has a proof independent of the general Riemann hypothesis being recovered [58, Introduction]. The reduction is substantial, and its explicit inclusion is essential to the claimed strength of the linchpin.

Finite fields can be described by finite addition and multiplication tables. Thus both the hypothesis over extensions and the conclusion can be stated using finite algebraic data, although the hypothesis quantifies over all finite extensions. The coarse constant in (10.2) was chosen to simplify the statement. A sharp Betti-number constant is unnecessary for the reverse implication.

10.2 Ramanujan's coefficients

Define integers $\tau(n)$ by the formal power series

$$t \prod_{j=1}^{\infty} (1 - t^j)^{24} = \sum_{n=1}^{\infty} \tau(n) t^n.$$

Each coefficient requires only finitely many factors.

Statement 10.2 (Ramanujan's inequality). *For every prime p ,*

$$\tau(p)^2 \leq 4p^{11}.$$

Status. A theorem downstream from Deligne’s Riemann hypothesis over finite fields [23, Theorem 8.2]. No converse is claimed.

The roots of $T^2 - \tau(p)T + p^{11}$ are realized in the appropriate degree of the cohomology of a Kuga–Sato variety. Deligne’s theorem gives absolute value $p^{11/2}$ for each root, and their sum is $\tau(p)$. The square in the displayed inequality removes the only real power from the usual statement. This is an example where a classical formulation already provides nearly all the desired simplification.

11 Birch and Swinnerton-Dyer

The original experiments of Birch and Swinnerton-Dyer concerned products of point counts. Their asymptotic conjecture preceded the modern formulation by the order of vanishing of an L -function [9, 10, 8]. That asymptotic gives a natural linchpin, provided its extra strength is stated explicitly.

11.1 Comparing finite-field and rational point counts

Fix $A, B \in \mathbb{Z}$ with $\Delta = -16(4A^3 + 27B^2) \neq 0$. For primes $p \nmid \Delta$, put

$$N_p = 1 + \#\{(x, y) \in \{0, \dots, p-1\}^2 : y^2 \equiv x^3 + Ax + B \pmod{p}\}.$$

For $x = u/v \in \mathbb{Q}$ in lowest terms, $v > 0$, define $H(x) = \max(|u|, v)$, and for $X \geq 1$ set

$$M_{A,B}(X) = 1 + \#\{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 + Ax + B, H(x) \leq X\}.$$

The added 1 counts the point at infinity.

Statement 11.1 (A point-count product). *For every such pair A, B , there is a real constant $C_{A,B} > 0$ such that*

$$\prod_{\substack{p \leq X \\ p \nmid \Delta}} \frac{N_p}{p} \sim C_{A,B} M_{A,B}(X)^2 \quad (X \rightarrow \infty). \quad (11.1)$$

Status. Open. This is a stronger conjectural formulation implying the rank part of BSD for every elliptic curve over $\mathbb{Q}$, and also the Riemann hypothesis for each of its L -functions. It is not known to follow from the modern rank conjecture alone.

For the elliptic curve $E : y^2 = x^3 + Ax + B$, let $r = \text{rank } E(\mathbb{Q})$. Mordell–Weil and the canonical height give, unconditionally,

$$M_{A,B}(X) \sim c_{A,B} (\log X)^{r/2}, \quad c_{A,B} > 0. \quad (11.2)$$

Indeed, modulo torsion the rational points form a lattice of rank r , and the canonical height is a positive definite quadratic form. The difference between $\log H(x)$ and twice the canonical height is bounded. Counting lattice points in expanding ellipsoids proves (11.2); see [60, Chapter VIII]. When $r = 0$, the count is eventually the size of the torsion group, so the same assertion holds with exponent zero.

Consequently (11.1) is equivalent to the historical product asymptotic

$$\prod_{\substack{p \leq X \\ p \nmid \Delta}} \frac{N_p}{p} \sim C'_{A,B} (\log X)^r, \quad C'_{A,B} > 0.$$

Omitting finitely many local factors changes only the constant. Goldfeld proved that such an asymptotic forces the exponent to be $\text{ord}_{s=1} L(E, s)$, and forces $L(E, s) \neq 0$ for $\Re s > 1$ [30]. Modularity of elliptic curves supplies the analytic continuation needed here [13]. Conrad gives the precise implication and analyzes the stronger convergence requirement [18, Theorems 1.1 and 1.3]. The functional equation then gives the elliptic-curve Riemann hypothesis. Combining the equality of exponents with (11.2) gives the rank conjecture.

The constant in (11.1) is unspecified. Thus this statement does not by itself express the refined BSD formula involving the regulator, periods, local factors, and the Tate–Shafarevich group. It is stronger in its analytic convergence assertion, while its stated arithmetic conclusion is the rank equality. These are separate comparisons of strength.

11.2 Rational right triangles

For positive integers c, d, m , let

$$R_{c,d}(m) = \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + cy^2 + dz^2 = m\}.$$

All signs and zero coordinates are included.

Statement 11.2 (A counting test for rational triangles). *Let n be a positive squarefree integer. There are $u, v, w \in \mathbb{Q}_{>0}$ such that*

$$u^2 + v^2 = w^2, \quad uv = 2n$$

if and only if

$$\begin{cases} R_{2,8}(n) = 2R_{2,32}(n), & n \text{ odd}, \\ R_{4,8}(n/2) = 2R_{4,32}(n/2), & n \text{ even}. \end{cases}$$

Status. The implication from a triangle to the count equality is unconditional. The converse follows from the rank conjecture for the curves $E_n : y^2 = x^3 - n^2x$, by Tunnell’s theorem [65]. The full biconditional remains a conditional downstream statement, not a theorem proved here.

A rational triangle of area n exists exactly when $E_n(\mathbb{Q})$ has positive rank. The elementary correspondence sends a rational point with $y \neq 0$ to side lengths

$$\left| \frac{x^2 - n^2}{y} \right|, \quad \left| \frac{2nx}{y} \right|, \quad \left| \frac{x^2 + n^2}{y} \right|.$$

Conversely, from a triangle one obtains $x = n(u + w)/v$, $y = 2n^2(u + w)/v^2$. The usual torsion calculation for E_n completes the positive-rank equivalence.

Tunnell identifies the vanishing of the relevant difference of representation counts with $L(E_n, 1) = 0$, using modular forms of weight $3/2$ and the central-value formula of Waldspurger [65, 66]. For the unconditional direction one also needs the theorem of Coates–Wiles for elliptic curves with complex multiplication [17]: if $L(E_n, 1) \neq 0$, then $E_n(\mathbb{Q})$ is finite. Each E_n has complex multiplication by $\mathbb{Z}[i]$. Thus a triangle gives positive rank, hence $L(E_n, 1) = 0$, and then the count equality. This dependency is explicit in [65, p. 325]. In the other direction, the count equality gives $L(E_n, 1) = 0$; rank BSD then gives positive rank and a triangle. More precisely, together with these established results, Statement 11.2 is equivalent to the assertion

$$\text{rank } E_n(\mathbb{Q}) > 0 \iff L(E_n, 1) = 0$$

for this family. It distinguishes rank zero from positive rank; it does not identify an arbitrary positive rank with the order of vanishing.

12 $P \neq NP$ by polynomial local updates

We use one-dimensional cellular automata because they are computationally universal, with polynomial time overhead for simulation by and of Turing machines [62, 46]. This preserves the distinction between polynomial and nonpolynomial time required here. “One-dimensional” refers to the line of cells; the local update need not be a linear function. Allowing the finite local rule to vary makes the input convention simple. The reduction below gives the polynomial simulations explicitly.

Fix a prime $p \geq 7$ and a polynomial $F \in \mathbb{F}_p[X, Y, Z]$ with $F(0, 0, 0) = 0$. For a sequence $z_i(t) \in \mathbb{F}_p$, indexed by $i \in \mathbb{Z}$, define

$$z_i(t+1) = F(z_{i-1}(t), z_i(t), z_{i+1}(t)). \quad (12.1)$$

This is a cellular automaton on a line, with a common rule at every position and time.

Let G be a simple graph on $[n]$, $n \geq 1$, with adjacency matrix (e_{uv}) . Start the recurrence with

$$\begin{aligned} z_0(0) &= 3, \\ z_{(u-1)n+v}(0) &= 1 + e_{uv} \quad (1 \leq u, v \leq n), \quad z_i(0) = 0 \quad \text{at every other position.} \\ z_{n^2+1}(0) &= 4, \end{aligned}$$

The symbols 3, 4 mark the input, 1, 2 encode its bits, and 0 is the blank symbol. A graph is 3-colorable if there is $\chi : [n] \rightarrow \{1, 2, 3\}$ with $\chi(u) \neq \chi(v)$ whenever $e_{uv} = 1$.

Statement 12.1 (No uniformly fast local coloring rule). *There do not exist a prime $p \geq 7$, a polynomial $F \in \mathbb{F}_p[X, Y, Z]$ with $F(0, 0, 0) = 0$, and positive integers c, k , such that for every $n \geq 1$ and every simple graph G on $[n]$, the recurrence above satisfies*

$$z_0(cn^k) = \begin{cases} 5, & G \text{ is 3-colorable,} \\ 6, & G \text{ is not 3-colorable.} \end{cases}$$

Status. Open; equivalent to $P \neq NP$. The connection uses established polynomial simulation and the NP-completeness of graph 3-colorability [19, 27, 62]. No additional conjecture is required.

Suppose the statement is false. The fixed rule uses a fixed finite field, so one update takes constant time in a conventional model of computation. At time T , only an interval of $O(n^2 + T)$ cells can have been affected, because a change travels at most one position per update and an all-zero neighborhood stays zero. Simulating $T = cn^k$ steps takes $O(T(n^2 + T))$ time. The rule therefore decides 3-colorability in polynomial time, and NP-completeness gives $P = NP$.

Conversely, assume $P = NP$. Take a deterministic polynomial-time procedure for graph 3-colorability. It can be implemented on a one-tape Turing machine with a left end and polynomial overhead. Encode each tape square by its symbol, together with a state marker if the head is present. The initial symbol 3 encodes both the left-end marker and the head in its initial state at position 0. The machine preserves the left-end marker; after the head leaves, that square retains a distinct unheaded marker state. Assign distinct labels at least 7 to all additional encoded states. The next state of a square depends only on it and its two neighbors: the head moves by at most one square. This is a nearest-neighbor cellular automaton with a fixed finite alphabet. After the decision, return the head to the marked initial square and write 5 or 6. Make these output states absorbing, as specified below, so that the answer persists until the prescribed time. These operations still take polynomial time. The prescribed input is a delimited adjacency matrix, whose length is $n^2 + 2$, so suitable c, k work for every n .

Choose a prime p large enough to encode all states, reserving $0, \dots, 6$ for the specified symbols. Extend the local rule f to unused states, requiring

$$f(a, 5, b) = 5, \quad f(a, 6, b) = 6 \quad \text{for all } a, b \in \mathbb{F}_p.$$

Apart from these requirements and the blank transition below, the extension is arbitrary. Every function $f : \mathbb{F}_p^3 \rightarrow \mathbb{F}_p$ is polynomial:

$$F(X, Y, Z) = \sum_{a, b, d \in \mathbb{F}_p} f(a, b, d) \delta_a(X) \delta_b(Y) \delta_d(Z), \quad \delta_a(X) = 1 - (X - a)^{p-1}.$$

Choose the blank transition to be $f(0, 0, 0) = 0$. This gives a polynomial satisfying all the requirements that Statement 12.1 denies.

The uniformity lies in the order of the quantifiers: p, F, c, k are chosen once for all graphs. Nothing depends on a separate circuit chosen for each input size. The recurrence is a model of computation, but its entire definition is the single polynomial update (12.1). Polynomial universality is also known for a fixed small rule such as Rule 110 [46]; using that rule would move additional complexity into the input encoding without simplifying the present statement.

13 Theorems that already have elementary statements

Two results obtained by large satisfiability computations need no substantial reformulation. Their statements make clear that the length of a proof and the complexity of its conclusion are different matters.

Statement 13.1 (Boolean Pythagorean triples). *Every map $\chi : [7825] \rightarrow \{0, 1\}$ has positive integers $a, b, c \leq 7825$ such that*

$$a^2 + b^2 = c^2, \quad \chi(a) = \chi(b) = \chi(c).$$

There exists a map $\chi : [7824] \rightarrow \{0, 1\}$ with no such triple.

Status. A theorem of Heule–Kullmann–Marek [35]. This is the original finite threshold theorem, used as its own linchpin. It implies the corresponding assertion for every two-coloring of the positive integers.

A formulation only about the infinite set of positive integers would omit the exact threshold. The finite statement includes both the obstruction and its sharpness.

Statement 13.2 (The fifth Schur number). *There exists a map $\chi : [160] \rightarrow \{1, 2, 3, 4, 5\}$ for which no $x, y, z \in [160]$ satisfy*

$$x + y = z, \quad \chi(x) = \chi(y) = \chi(z).$$

Every map $\chi : [161] \rightarrow \{1, 2, 3, 4, 5\}$ has such a triple.

Status. The theorem $S(5) = 160$, proved by Heule [34]. It is already an elementary linchpin statement.

The variables x, y, z need not be pairwise distinct; in particular $x = y$ is allowed. This convention is essential to the definition of the Schur number. The first assertion is a finite witness, and the second is a finite universal claim. The computations in [35, 34] produce checkable certificates. In a formal audit one must also connect the coloring statement to the encoded satisfiability problem and verify the certificate checker. A large certificate does not remove this semantic obligation.

14 Using the linchpins

The examples separate three questions. Is the statement easy to understand? What is its mathematical relation to the source theorem? Does the particular formal proof test the mathematics that the auditor intended to test? A good answer to the first question does not settle the other two.

Equivalent formulations offer the strongest protection against an accidental loss of content. The Kepler and Poincaré examples illustrate two different mechanisms: a packing can be inserted into a periodic configuration, and an arbitrary three-manifold can be represented by integer equations. The hypersurface example requires a much deeper bridge. Its elementary counting statement retains the full Riemann hypothesis over finite fields only because Scholl’s theorem is part of the connection.

Downstream statements may be more convenient, but they require an explicit decision about how much of the source is being tested. The six-entry rearrangement statement does not reconstruct CFSG. Twelve-square counts test an application of the unitary fundamental lemma. The weighted filling statement has a published proof route through Almgren regularity, yet may permit a bypass. These qualifications are part of the specification of an audit.

A formal development should expose the chosen statement, its definitions, its premises, and the bridge that invokes the source theorem. A human should be able to read that interface without reconstructing the entire development. If a successful proof leaves the intended source untouched, the appropriate response is to reconsider the linchpin. The objective remains the audit of mathematics, rather than the preservation of a particular list of statements.

AI statement. ChatGPT-6 Astra generated this document on October 16, 2026 at the prompting of Thomas Hales.

References

- [1] F. J. Almgren, Jr., *Almgren’s Big Regularity Paper: Q -Valued Functions Minimizing Dirichlet’s Integral and the Regularity of Area-Minimizing Rectifiable Currents up to Codimension 2*, edited by V. Scheffer and J. E. Taylor, World Scientific Monograph Series in Mathematics, vol. 1, World Scientific, 2000.
- [2] L. Ambrosio, N. Fusco, and D. Pallara, *Functions of Bounded Variation and Free Discontinuity Problems*, Oxford Mathematical Monographs, Oxford University Press, 2000. [doi:10.1093/oso/9780198502456.001.0001](https://doi.org/10.1093/oso/9780198502456.001.0001).
- [3] J. Araújo, W. Bentz, and P. J. Cameron, The existential transversal property: a generalization of homogeneity and its impact on semigroups, *Trans. Amer. Math. Soc.* **374** (2021), 1155–1195. [doi:10.1090/tran/8285](https://doi.org/10.1090/tran/8285).
- [4] L. Báez-Duarte, A strengthening of the Nyman–Beurling criterion for the Riemann hypothesis, *Rend. Lincei Mat. Appl.* (9) **14** (2003), 5–11. [arXiv:math/0202141](https://arxiv.org/abs/math/0202141).
- [5] B. Bagchi, On Nyman, Beurling and Baez-Duarte’s Hilbert space reformulation of the Riemann hypothesis, *Proc. Indian Acad. Sci. Math. Sci.* **116** (2006), 137–146. [doi:10.1007/BF02829783](https://doi.org/10.1007/BF02829783).
- [6] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor, A family of Calabi–Yau varieties and potential automorphy II, *Publ. Res. Inst. Math. Sci.* **47** (2011), 29–98. [doi:10.2977/PRIMS/31](https://doi.org/10.2977/PRIMS/31).
- [7] A. Beurling, A closure problem related to the Riemann zeta-function, *Proc. Natl. Acad. Sci. USA* **41** (1955), 312–314. [doi:10.1073/pnas.41.5.312](https://doi.org/10.1073/pnas.41.5.312).

- [8] B. J. Birch, Conjectures concerning elliptic curves, in *Arithmetic Algebraic Geometry*, Proc. Sympos. Pure Math., vol. 8, American Mathematical Society, 1965, pp. 106–112.
- [9] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves. I, *J. Reine Angew. Math.* **212** (1963), 7–25. [doi:10.1515/crll.1963.212.7](https://doi.org/10.1515/crll.1963.212.7).
- [10] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves. II, *J. Reine Angew. Math.* **218** (1965), 79–108. [doi:10.1515/crll.1965.218.79](https://doi.org/10.1515/crll.1965.218.79).
- [11] A. Borel, Some remarks about Lie groups transitive on spheres and tori, *Bull. Amer. Math. Soc.* **55** (1949), 580–587. [doi:10.1090/S0002-9904-1949-09251-0](https://doi.org/10.1090/S0002-9904-1949-09251-0).
- [12] A. Borisov, Quotient singularities, integer ratios of factorials, and the Riemann hypothesis, *Int. Math. Res. Not.* **2008**, article rnn052. [doi:10.1093/imrn/rnn052](https://doi.org/10.1093/imrn/rnn052).
- [13] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.
- [14] M. R. Bridson and A. Haefliger, *Metric Spaces of Non-Positive Curvature*, Grundlehren der mathematischen Wissenschaften, vol. 319, Springer, 1999. [doi:10.1007/978-3-662-12494-9](https://doi.org/10.1007/978-3-662-12494-9).
- [15] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, 1999.
- [16] A. Chambolle, L. A. D. Ferrari, and B. Merlet, Strong approximation in h -mass of rectifiable currents under homological constraint, *Adv. Calc. Var.* **14** (2021), 343–363. [doi:10.1515/acv-2018-0079](https://doi.org/10.1515/acv-2018-0079).
- [17] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251. [doi:10.1007/BF01402975](https://doi.org/10.1007/BF01402975).
- [18] K. Conrad, Partial Euler products on the critical line, *Canad. J. Math.* **57** (2005), 267–297. [doi:10.4153/CJM-2005-012-6](https://doi.org/10.4153/CJM-2005-012-6).
- [19] S. A. Cook, The complexity of theorem-proving procedures, in *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, ACM, 1971, pp. 151–158. [doi:10.1145/800157.805047](https://doi.org/10.1145/800157.805047).
- [20] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, second ed., Wiley, 2013.
- [21] A. J. de Jong, Smoothness, semi-stability and alterations, *Publ. Math. Inst. Hautes Études Sci.* **83** (1996), 51–93. [doi:10.1007/BF02698644](https://doi.org/10.1007/BF02698644).
- [22] A. J. de Jong, Families of curves and alterations, *Ann. Inst. Fourier (Grenoble)* **47** (1997), 599–621. [doi:10.5802/aif.1575](https://doi.org/10.5802/aif.1575).
- [23] P. Deligne, La conjecture de Weil. I, *Publ. Math. Inst. Hautes Études Sci.* **43** (1974), 273–307. [Numdam](https://numdam.org/).
- [24] P. Deligne, La conjecture de Weil. II, *Publ. Math. Inst. Hautes Études Sci.* **52** (1980), 137–252. [Numdam](https://numdam.org/).

- [25] H. Federer, *Geometric Measure Theory*, Grundlehren der mathematischen Wissenschaften, vol. 153, Springer, 1969.
- [26] B. Fein, W. M. Kantor, and M. Schacher, Relative Brauer groups. II, *J. Reine Angew. Math.* **328** (1981), 39–57. [doi:10.1515/crll.1981.328.39](https://doi.org/10.1515/crll.1981.328.39).
- [27] M. R. Garey, D. S. Johnson, and L. Stockmeyer, Some simplified NP-complete graph problems, *Theoret. Comput. Sci.* **1** (1976), 237–267. [doi:10.1016/0304-3975\(76\)90059-1](https://doi.org/10.1016/0304-3975(76)90059-1).
- [28] R. Ghiloni and E. Savi, The Nash–Tognoli theorem over the rationals and its version for isolated singularities, preprint, 2023, revised 2025. [arXiv:2302.04142v4](https://arxiv.org/abs/2302.04142v4).
- [29] S. R. Ghorpade and G. Lachaud, Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, *Mosc. Math. J.* **2** (2002), 589–631; corrected version, [arXiv:0808.2169](https://arxiv.org/abs/0808.2169).
- [30] D. Goldfeld, Sur les produits partiels eulériens attachés aux courbes elliptiques, *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982), 471–474.
- [31] T. C. Hales, The work of Ngô Bao Châu, *Notices Amer. Math. Soc.* **58** (2011), 453–458. [arXiv:1012.0382](https://arxiv.org/abs/1012.0382).
- [32] T. Hales, M. Adams, G. Bauer, T. D. Dang, J. Harrison, L. T. Hoang, C. Kaliszyk, V. Magron, S. McLaughlin, T. T. Nguyen, Q. T. Nguyen, T. Nipkow, S. Obua, J. Pleso, J. Rute, A. Solovyev, T. H. A. Ta, N. T. Tran, T. D. Trieu, J. Urban, K. Vu, and R. Zumkeller, A formal proof of the Kepler conjecture, *Forum Math. Pi* **5** (2017), e2, 29 pp. [doi:10.1017/fmp.2017.1](https://doi.org/10.1017/fmp.2017.1).
- [33] M. Harris, N. Shepherd-Barron, and R. Taylor, A family of Calabi–Yau varieties and potential automorphy, *Ann. of Math. (2)* **171** (2010), 779–813. [doi:10.4007/annals.2010.171.779](https://doi.org/10.4007/annals.2010.171.779).
- [34] M. J. H. Heule, Schur number five, in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 32, 2018, pp. 6598–6606. [doi:10.1609/aaai.v32i1.12209](https://doi.org/10.1609/aaai.v32i1.12209).
- [35] M. J. H. Heule, O. Kullmann, and V. W. Marek, Solving and verifying the Boolean Pythagorean triples problem via cube-and-conquer, in *Theory and Applications of Satisfiability Testing—SAT 2016*, Lecture Notes in Computer Science, vol. 9710, Springer, 2016, pp. 228–245. [doi:10.1007/978-3-319-40970-2_15](https://doi.org/10.1007/978-3-319-40970-2_15).
- [36] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Texts in Mathematics, vol. 9, Springer, 1972.
- [37] A. W. Knap, *Lie Groups Beyond an Introduction*, second ed., Progress in Mathematics, vol. 140, Birkhäuser, 2002.
- [38] J. C. Lagarias, An elementary problem equivalent to the Riemann hypothesis, *Amer. Math. Monthly* **109** (2002), 534–543. [doi:10.1080/00029890.2002.11919883](https://doi.org/10.1080/00029890.2002.11919883).
- [39] G. Laumon and B.-C. Ngô, Le lemme fondamental pour les groupes unitaires, *Ann. of Math. (2)* **168** (2008), 477–573. [doi:10.4007/annals.2008.168.477](https://doi.org/10.4007/annals.2008.168.477).
- [40] J. E. Littlewood, Quelques conséquences de l’hypothèse que la fonction $\zeta(s)$ de Riemann n’a pas de zéros dans le demi-plan $\Re s > 1/2$, *C. R. Acad. Sci. Paris* **154** (1912), 263–266.

- [41] K. Madlener, S. Smetsers, and M. van Eekelen, A formal verification study on the Rotterdam storm surge barrier, in *Formal Methods and Software Engineering—ICFEM 2010*, Lecture Notes in Computer Science, vol. 6447, Springer, 2010, pp. 287–302. [doi:10.1007/978-3-642-16901-4_20](https://doi.org/10.1007/978-3-642-16901-4_20).
- [42] J. Milnor, *Morse Theory*, Annals of Mathematics Studies, vol. 51, Princeton University Press, 1963.
- [43] N. I. S. Mohammad and T. Sheikh, The faithfulness gap: certifying semantic equivalence between natural-language and formal mathematical statements, preprint, 2026. [arXiv:2606.16541](https://arxiv.org/abs/2606.16541).
- [44] E. E. Moise, *Geometric Topology in Dimensions 2 and 3*, Graduate Texts in Mathematics, vol. 47, Springer, 1977.
- [45] J. Morgan and G. Tian, *Ricci Flow and the Poincaré Conjecture*, Clay Mathematics Monographs, vol. 3, American Mathematical Society and Clay Mathematics Institute, 2007.
- [46] T. Neary and D. Woods, P-completeness of cellular automaton Rule 110, in *Automata, Languages and Programming—ICALP 2006*, Lecture Notes in Computer Science, vol. 4051, Springer, 2006, pp. 132–143. [doi:10.1007/11786986_13](https://doi.org/10.1007/11786986_13).
- [47] B.-C. Ngô, Le lemme fondamental pour les algèbres de Lie, *Publ. Math. Inst. Hautes Études Sci.* **111** (2010), 1–169. [doi:10.1007/s10240-010-0026-7](https://doi.org/10.1007/s10240-010-0026-7).
- [48] B. Nyman, *On Some Groups and Semigroups of Translations*, doctoral thesis, Uppsala University, 1950.
- [49] B. O’Neill, *Semi-Riemannian Geometry with Applications to Relativity*, Pure and Applied Mathematics, vol. 103, Academic Press, 1983.
- [50] G. Perelman, The entropy formula for the Ricci flow and its geometric applications, preprint, 2002. [arXiv:math/0211159](https://arxiv.org/abs/math/0211159).
- [51] G. Perelman, Ricci flow with surgery on three-manifolds, preprint, 2003. [arXiv:math/0303109](https://arxiv.org/abs/math/0303109).
- [52] G. Perelman, Finite extinction time for the solutions to the Ricci flow on certain three-manifolds, preprint, 2003. [arXiv:math/0307245](https://arxiv.org/abs/math/0307245).
- [53] R. Pollack, How to believe a machine-checked proof, in G. Sambin and J. Smith (eds.), *Twenty Five Years of Constructive Type Theory*, Oxford University Press, 1998, pp. 205–220. Preprint: BRICS Report RS-97-18, 1997, [doi:10.7146/brics.v4i18.18945](https://doi.org/10.7146/brics.v4i18.18945).
- [54] M. Rapoport and T. Zink, Über die lokale Zetafunktion von Shimuravarietäten. Monodromiefiltration und verschwindende Zyklen in ungleicher Charakteristik, *Invent. Math.* **68** (1982), 21–101. [doi:10.1007/BF01394268](https://doi.org/10.1007/BF01394268).
- [55] Yu. G. Reshetnyak, The weak convergence of completely additive vector-valued set functions, *Siberian Math. J.* **9** (1968), 1039–1045. [doi:10.1007/BF02196453](https://doi.org/10.1007/BF02196453).
- [56] G. Robin, Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann, *J. Math. Pures Appl.* (9) **63** (1984), 187–213.

- [57] J. Rushby, *Formal Methods and their Role in the Certification of Critical Systems*, Technical Report SRI-CSL-95-1, Computer Science Laboratory, SRI International, 1995. Also issued as NASA Contractor Report 4673 under the title *Formal Methods and Their Role in Digital Systems Validation for Airborne Systems*. [NASA report](#).
- [58] A. J. Scholl, Hypersurfaces and the Weil conjectures, *Int. Math. Res. Not.* **2011**, no. 5, 1010–1022. [doi:10.1093/imrn/rnq098](#).
- [59] F. Schulze, Optimal isoperimetric inequalities for surfaces in any codimension in Cartan–Hadamard manifolds, *Geom. Funct. Anal.* **30** (2020), 255–288. [doi:10.1007/s00039-020-00522-8](#).
- [60] J. H. Silverman, *The Arithmetic of Elliptic Curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009.
- [61] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.
- [62] A. R. Smith III, Real-time language recognition by one-dimensional cellular automata, *J. Comput. System Sci.* **6** (1972), 233–253. [doi:10.1016/S0022-0000\(72\)80004-7](#).
- [63] K. Soundararajan, Partial sums of the Möbius function, *J. Reine Angew. Math.* **631** (2009), 141–152. [doi:10.1515/CRELLE.2009.044](#).
- [64] A. Topaz, Definitions in the liquid tensor experiment, *Lean community blog*, 14 October 2022. [Online article](#).
- [65] J. B. Tunnell, A classical Diophantine problem and modular forms of weight $3/2$, *Invent. Math.* **72** (1983), 323–334. [doi:10.1007/BF01389327](#).
- [66] J.-L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, *J. Math. Pures Appl.* (9) **60** (1981), 375–484.
- [67] J.-L. Waldspurger, Endoscopie et changement de caractéristique, *J. Inst. Math. Jussieu* **5** (2006), 423–525.
- [68] Y. Wu, A. Q. Jiang, W. Li, M. N. Rabe, C. Staats, M. Jamnik, and C. Szegedy, Autoformalization with large language models, *Advances in Neural Information Processing Systems* **35** (2022), 32353–32368. [arXiv:2205.12615](#).