Justin Clarke-Doane
Columbia University

Proof and Agreement in Mathematics

- Riehl's excellent discussion is a chapter in the ancient debate about proof.
    - *Macbeth*: '[T]o…Plato, Descartes, and [their followers] the virtue of a (successful) train of…thought lies in the **insight and understanding** it affords. For…Aristotle, Leibniz, and [others – especially, Frege and Russell] it lies…in the power of the train of thought to show indubitably that some theorem is true and thereby to **end once and for all disagreements** as to its truth (2021, 9).'

- A **Platonic** proof is an argument that shows *why* the claim proved *must* be true; an **Aristotelian** proof is an argument that could be checked by a computer, without any knowledge of the meanings of the symbols involved. Although there can be proofs that are both Platonic and Aristotelian, almost all mathematical proofs of interest are merely Platonic. But Riehl shares the common view that they answer to Aristotelian proofs.

- *The Central Dogma of Mathematical Formalism* (Harris): An alleged mathematical proof is valid **if and only if** it 'indicates' the existence of a valid Aristotelian proof (understood as a finite sequence of symbols, each line of which is either an axiom – traditionally of *ZFC* set theory + small large cardinals – or follows from a previous line by a rule of formal inference, the last line of which is – a formal version of! – the claim to be proved).
    - *Note*: How to understand 'indicates' here is vexed!

- The *only if* direction is very hard to deny. Consider Gödel's and Cohen's arguments that $Con(ZFC) \rightarrow Con(ZFC + CH)$ and $Con(ZFC) \rightarrow Con(ZFC + \sim CH)$. These arguments strictly show that that there is no *formal* proof of a formal statement of the Continuum Hypothesis (*CH*) or its negation from a formal statement of Zermelo-Fraenkel set theory with the Axiom of Choice (*ZFC*), if that theory is formally (!) consistent. Nevertheless, such independence results are widely agreed to establish that anyone seeking to prove *CH* or ~*CH*, in the ordinary, Platonic, sense is wasting their time. (Some theorists, like Woodin, hope to identify *new axioms* that settle *CH*. But that just confirms the point.)

- The *if* direction is more debatable. One worry is that 'We cannot possibly achieve…the essential element of proof – our own personal understanding – if part of the argument is hidden away in a box' [as it is in the 'proof' of computer assisted proofs] (Bonsall 1987, 599).' But understanding comes in degrees. Although we cannot survey all the cases in the proof of the Kepler conjecture, say, we can 'communicate [the proof] in…a natural language… and…vett' it in an everyday sense. Another concern is that reliance on computers 'brings with it…the fallibility inherent in any physical science', as 'computers are just physical structures' (Tymoczko 1987, 600). However, mathematics *is* fallible!

- Is anything else required of a purported proof? Riehl 'propose[s] the following norm' to cover computer proofs, in particular: *Any artificially generated mathematical text will not be considered as a proof unless: It has been communicated in both a natural language text paired with a computer formalization of all definitions, theorems, and proofs. [and] The formalization has been accepted by the proof assistant and human expert referees have vetted both the formalization and the paired text.*' This is not a **conceptual analysis** of 'proof' (compare: the – extensionally equivalent – analyses of *computability*). It is a **policy position**. Riehl observes that our notion of proof has transformed, and this process is likely to continue. So, it seems more interesting to ask what arguments we *ought* to accept – not which ones count as 'proofs' according to the standards that we have inherited. We might understand the *Central Dogma* correlatively – not as a descriptive claim – whether one of conceptual analysis or not – but as a policy position.

- Let me conclude with Riehl's question: *Why has mathematics largely avoided the replication crisis…?* More generally, why is there *so little disagreement* in mathematics?

- No doubt 'careful refereeing' and 'careful[ness] in claiming [to] have a proof' are part of the story, as Riehl observes. But I wonder if the mystery does not run deeper than that.

- Distinguish three claims over which mathematicians might be supposed to agree:

    1. There are infinitely-many prime numbers.

    2. It follows from the Peano Axioms (so certainly from *ZFC* + small large cardinals!) that there are infinitely-many prime numbers.

    3. It follows in classical logic from the Peano Axioms that there are infinitely-many prime numbers.

- When mathematicians agree to Euclid's Theorem, over which of (1) – (3) do they concur? Perhaps they agree over the theorem itself – i.e., over (1). But that would be bold! Do they know something that the physicists do not about the number of objects in the world? It is more charitable to suppose that mathematicians agree over (2). But that suggests that they agree as to *which logic is correct*. Have typical mathematicians (unlike the ones here!) even taken a position on this question? Perhaps the most promising suggestion is that they agree over (3). Whether one is a predicativist or a finitist, classicist or intuitionist, we can agree on what follows form what in a logic. Right? Not always! What follows from what *in a logic* can turn on the logic that you use to check.[1]

[1] This is clear in the case of higher-order consequence relations lacking sound and complete proof systems. It is also true if we consider disagreement over the standard model of arithmetic, $\mathbb{N}$, e.g., one according to which there is a number coding a proof of '0 = 1' from the Peano Axioms and another in which there is not. If we consider *ultrafinitist* systems where extremely large numerals do not denote, we can even arrange for disagreement over the Δ_0 claim that a particular finite string *is* a proof-in-classical-logic (not just that there exists such a proof). In fact, there is a more familiar way to do this (Shapiro 2014, Ch. 6). Fix the object-logic CA_3, Priest's inconsistent arithmetic with *LP* as its underlying logic (Priest 1987). In CA_3 there are true contradictions, even among decidable arithmetic identities. Let CA_1 be a classical meta-theory (ordinary classical arithmetic), and CA_3 (the same inconsistent arithmetic used as a meta-theory). Let G be the diagonal (Gödel) sentence satisfying, in CA_3, G ↔

- *Upshot*: If consensus – even over what follows from what in a fixed logic! – depends on prior agreement over (meta-)logic, and (meta-)logic is subject to endless philosophical controversy, then mathematical agreement may be more mysterious than Riehl lets on.

Works Cited

Bonsall, F.F. "Computer Proofs" in Fauvel, John and Jeremy Gray. (1987) *The History of Mathematics: A Reader*. Macmillan.
Harris, Michael. (2022) "The Central Dogma of Mathematical Formalism." *Silicon Reckoner.* January 19. https://siliconreckoner.substack.com/p/the-central-dogma-of-mathematical
Macbeth, Danielle. (2021) "Formal Proofs in Mathematical Practice." in Bharath Sriraman (ed.), *Handbook of the History and Philosophy of Mathematical Practice*. Springer.
Priest, Graham. (1987) *In Contradiction*. Oxford University Press.
Shapiro, Stewart. (2014) Varieties of Logic. Oxford University Press.
Tymozco, Thomas. "Computer Proofs (contd.)" in Fauvel, John and Jeremy Gray. (1987) *The History of Mathematics: A Reader*. Macmillan.

$\neg$T(G, CA_3). Priest reports that both G and $\neg$G are derivable in CA_3, and, classically, one can verify the existence of those derivations. Hence, $CA_1 \vdash$ T(G, CA_3) and $CA_1 \vdash$ T($\neg$G, CA_3). But CA_3 is also supposed to prove both T(G, CA_3) and $\neg$T(G, CA_3), while the classicist rejects $\neg$T(G, CA_3). So: (1) There is a CA_3-derivation Π of G; (2) "Π is a CA_3-derivation of G" is a Δ_0 decidable property of the code $\ulcorner \Pi \urcorner$, and "$\exists$p Prov_CA_3(p, $\varnothing \vdash$ G)" is Σ_1; (3) CA_1 proves $\exists$p Prov_CA_3(p, $\varnothing \vdash$ G). However, (1)' In CA_3, G $\leftrightarrow$ $\neg$T(G, CA_3) [I assume that Priest's system incorporates a reasonable conditional according to which *MP* is valid]; (2)' $CA_3 \vdash$ G; hence (3) $CA_3 \vdash \neg$T(G, CA_3). (To be clear: the point is *not* that disagreement over ultrafinitism or inconsistent arithmetic is common. The point is: what explains why it is not? Not proof, since that requires prior agreement on metatheory!)