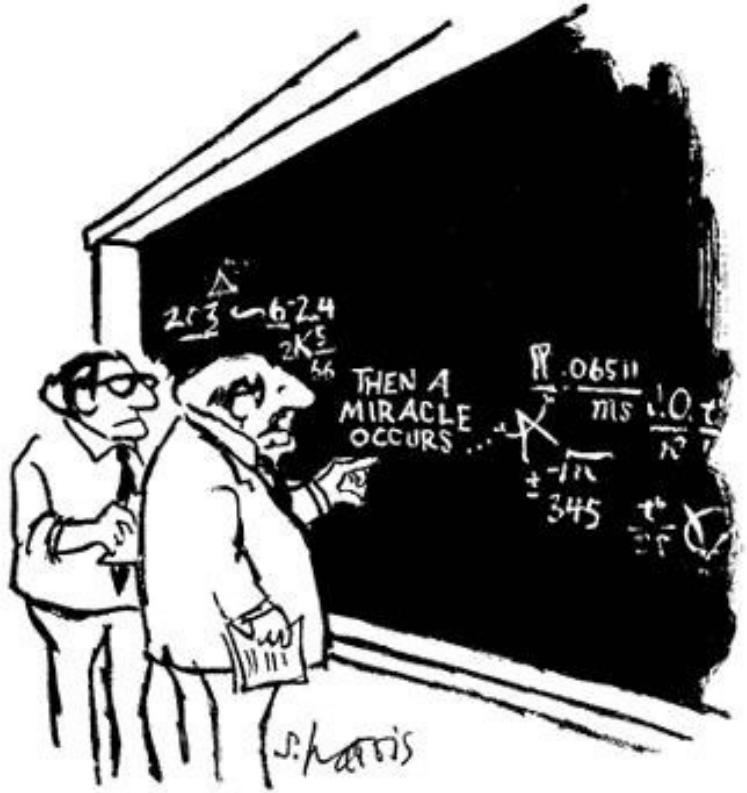
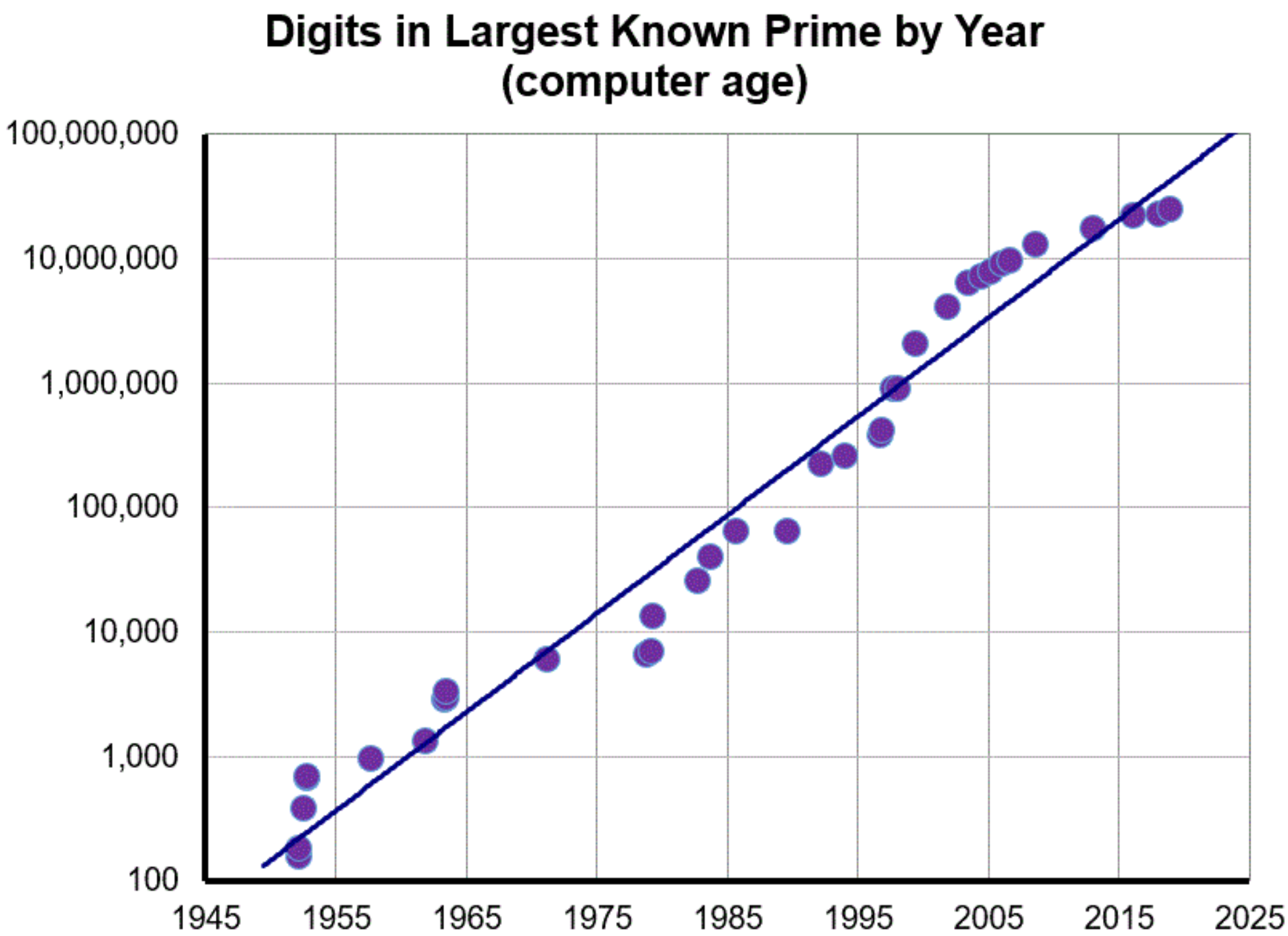


"I think you should be more explicit here in step two."

What's So Special About Deductive Proof?

Don Fallis

Northeastern University

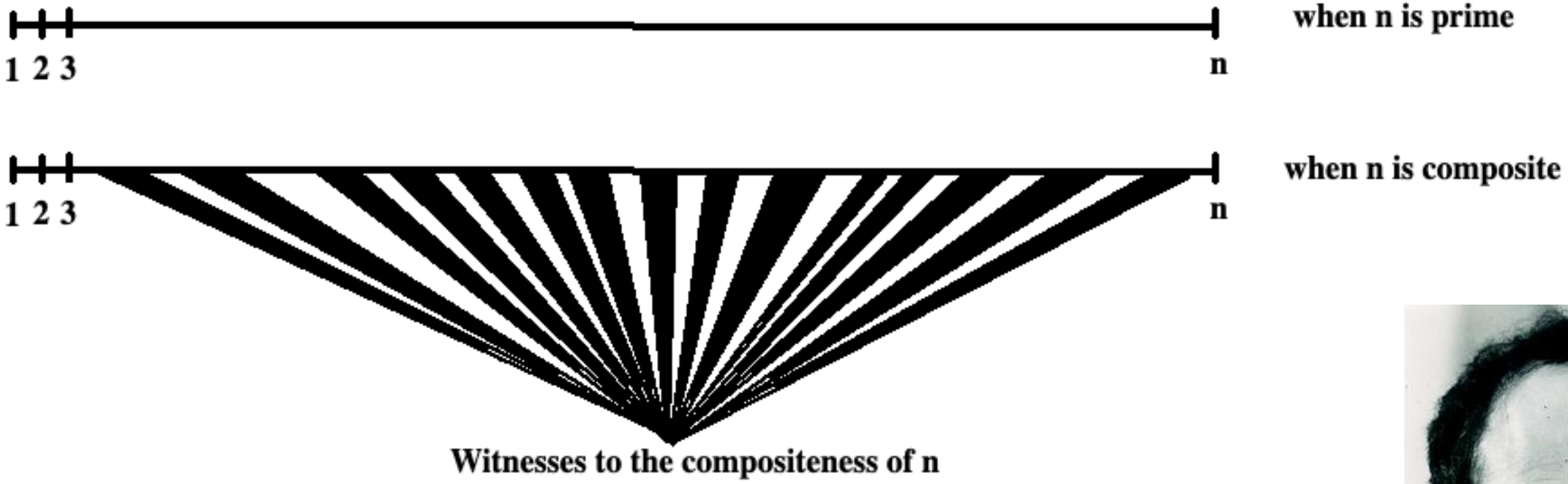

Digits in Largest Known Prime by Year
(computer age)
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
100
1945
1955
1965
1975
1985
1995
2005
2015
2025

Deductive Proof in Mathematics

- ***Theorem:*** There are more primes than found in any finite list of primes.
- ***Proof:*** Call the primes in our finite list p_1, p_2, ..., p_r. Let p be any common multiple of these primes plus one (for example, $p = p_1p_2...p_r+1$). Now p is either prime or it is not. If it is prime, then p is a prime that was not in our list. If p is not prime, then it is divisible by some prime, call it q. Notice q cannot be any of p_1, p_2, ..., p_r, otherwise q would divide 1, which is impossible. So this prime q is some prime that was not in our original list. Either way, the original list was incomplete.

Probabilistic Methods in Mathematics

Witnesses to Compositeness



- *a* is a ***witness to the compositeness*** of *n* if the following two conditions hold:
- (Note that, since *n* - 1 is even, it can be written as $d \times 2^s$ where *d* is odd and *s* > 1.)
  - $a^d \not\equiv 1 \pmod{n}$
  - $a^{d \times 2^r} \not\equiv -1 \pmod{n}$ for all $0 \le r < s$

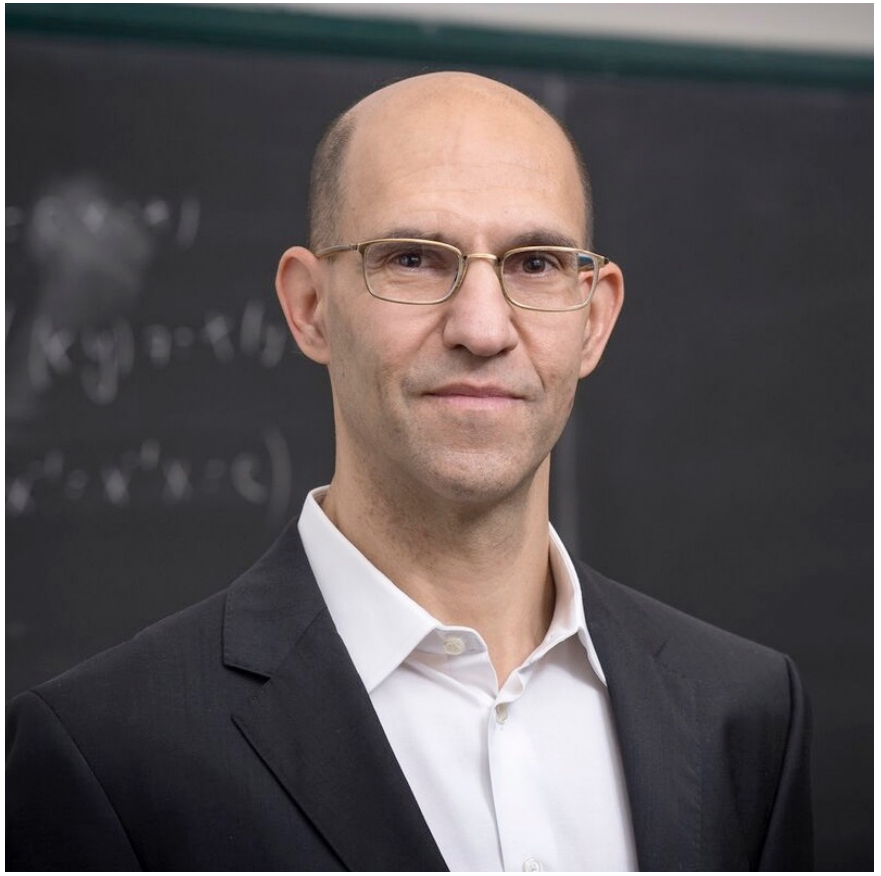
Rabin's Probabilistic Method

- Pick *k* numbers between 1 and *n* - 1 at random …
- For each of these *k* numbers …
  - Check whether it is a witness to the compositeness of *n*.
  - If it is, report "*n* is composite" and terminate.
  - Otherwise, continue with the loop.
- Report "*n* is prime" and terminate.

- If *n* is composite, the probability that none of the *k* randomly chosen numbers are witnesses is less than $(¼)^k$. So, for example, in order for that probability to be less than 0.1%, we just need to test 5 numbers.

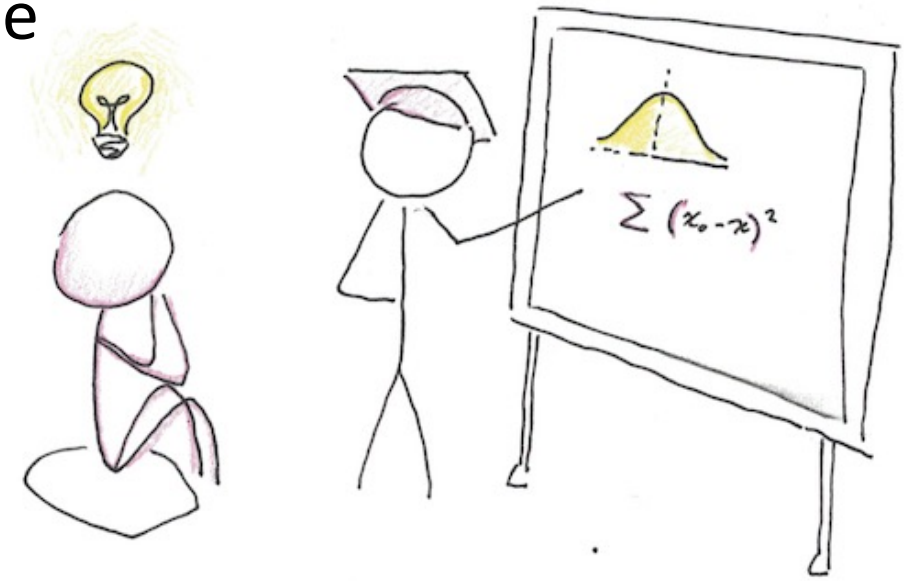
Avigad on the Right Sort of Thing

- “Fallis wonders why mathematicians refuse to admit inductive evidence in mathematical proofs. The easy answer to Fallis’ bemusement is simply that inductive evidence is not the right sort of thing to provide mathematical knowledge, as it is commonly understood.”



Provides Explanation?

- ***Theorem:*** 2 is the only even prime.
- ***Proof:*** Suppose that there is an even prime $p > 2$. Since p is even, it can be written as $p = 2q$ for some integer $q > 1$. But this means that p is composite, which contradicts our assumption that there is an even prime greater than 2.



Trial Division Method

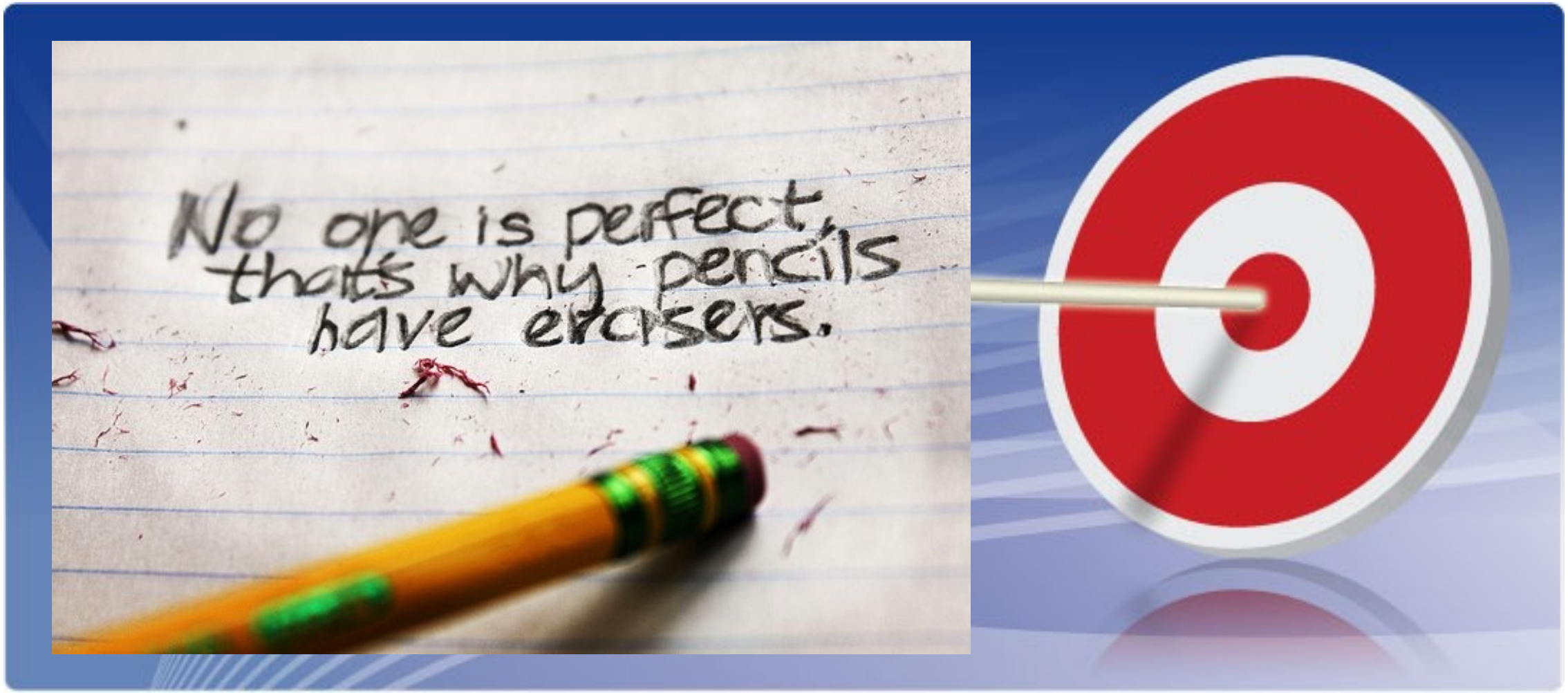
- For all integers *m* between 2 and *n* – 1 …
  - Divide *n* by *m*.
  - If there is no remainder, report “*n* is composite” and terminate.
  - Otherwise, continue with the loop.
- Report “*n* is prime” and terminate.

My Old Strategy

- In order to show why Rabin's probabilistic method should not be used to establish the truth of mathematical claims, we need to identify a property **P** such that:

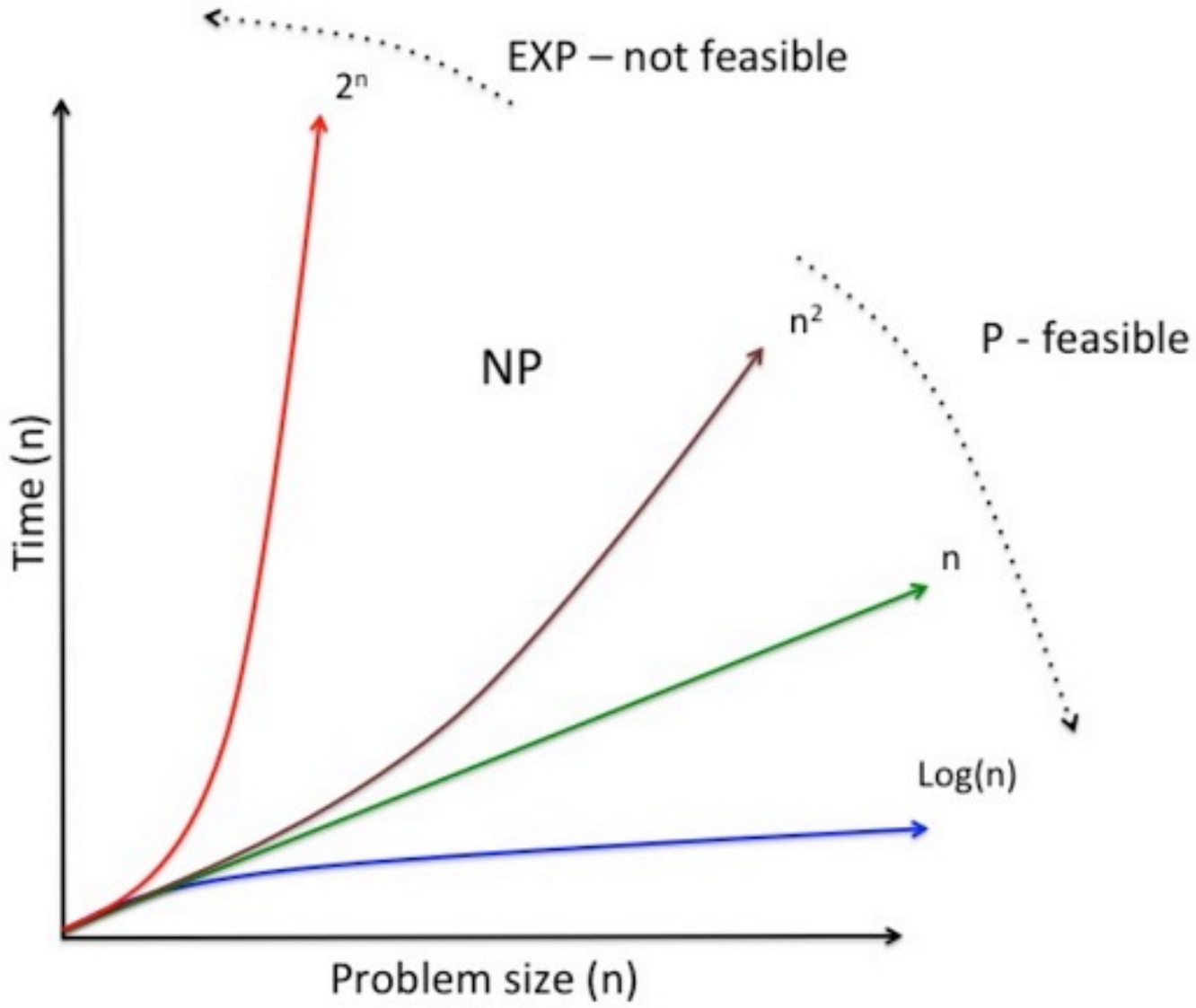
- Deductive proof *always* has property **P**.
  - In particular, the Trial Division method has property **P**.
- Rabin's probabilistic method does not have property **P**.
- Property **P** is epistemically valuable.

Provides Absolute Certainty?



Is More Reliable?

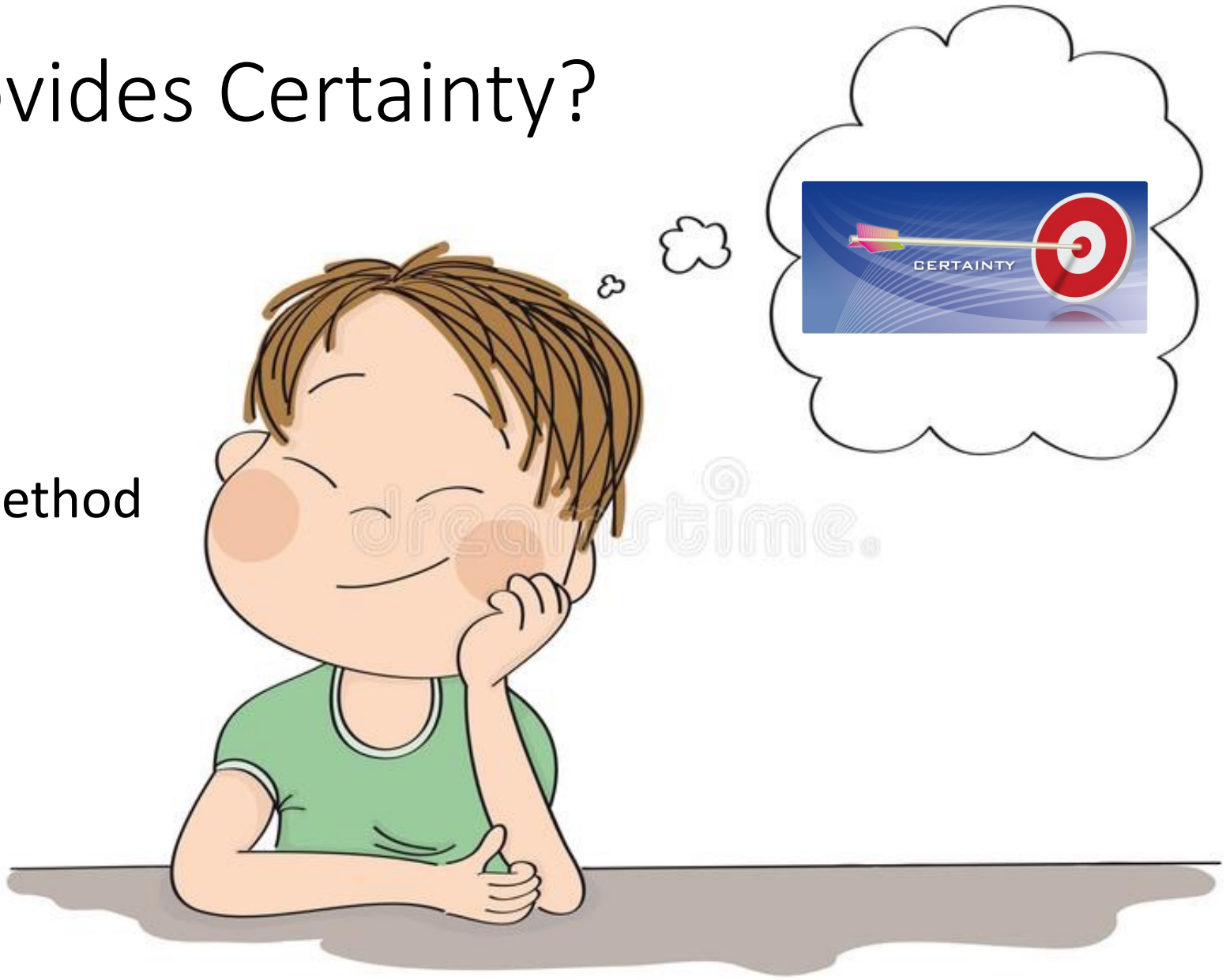
- Trial Division Method
  - Calculation Errors
- Rabin's Probabilistic Method
  - Calculation Errors
  - Probabilistic Errors



In Principle, Provides Certainty?

- Trial Division Method
  - ~~• Calculation Errors~~

- Rabin's Probabilistic Method
  - ~~• Calculation Errors~~
  - Probabilistic Errors



New Proposals in the Philosophy Literature

- Easwaran (2009) on Transferability
- Smith (2016) on Normic Support
- Berry (2019) on Univocality
- Hamami (forthcoming) on Finite Convergence

My New Strategy

- Deductive proof always has property **P**.
- Rabin's probabilistic method lacks property **P**.
- Property **P** is actually epistemically valuable.
  - Most notably, property **P** helps to account for why deductive proof is as *reliable* as it is.
- But Rabin's probabilistic method promotes the same epistemic value (or values) to at least as high a degree.
- Thus, property **P** does not show why Rabin's probabilistic method should not be used to establish the truth of mathematical claims.

Easwaran on Transferability

- “A proof is *transferable* just in case the sequence of propositions itself constitutes the proof … That is, mere consideration of the proposition suffices for a relevant expert to become convinced of the conclusion, unlike arguments in which one needs to know that certain propositions were generated in a suitably random manner.”

Why is Transferability Valuable?

- It enhances reliability.
  - It rules out *a potential source* of error.
- It enhances reliability *in the long run*.
  - It facilitates finding other errors.
- It promotes epistemic autonomy.

Smith on Normic Support

- “Say that a body of evidence E *normically supports* a proposition P just in case the circumstance in which E is true and P is false requires more explanation than the circumstance in which E and P are both true.”

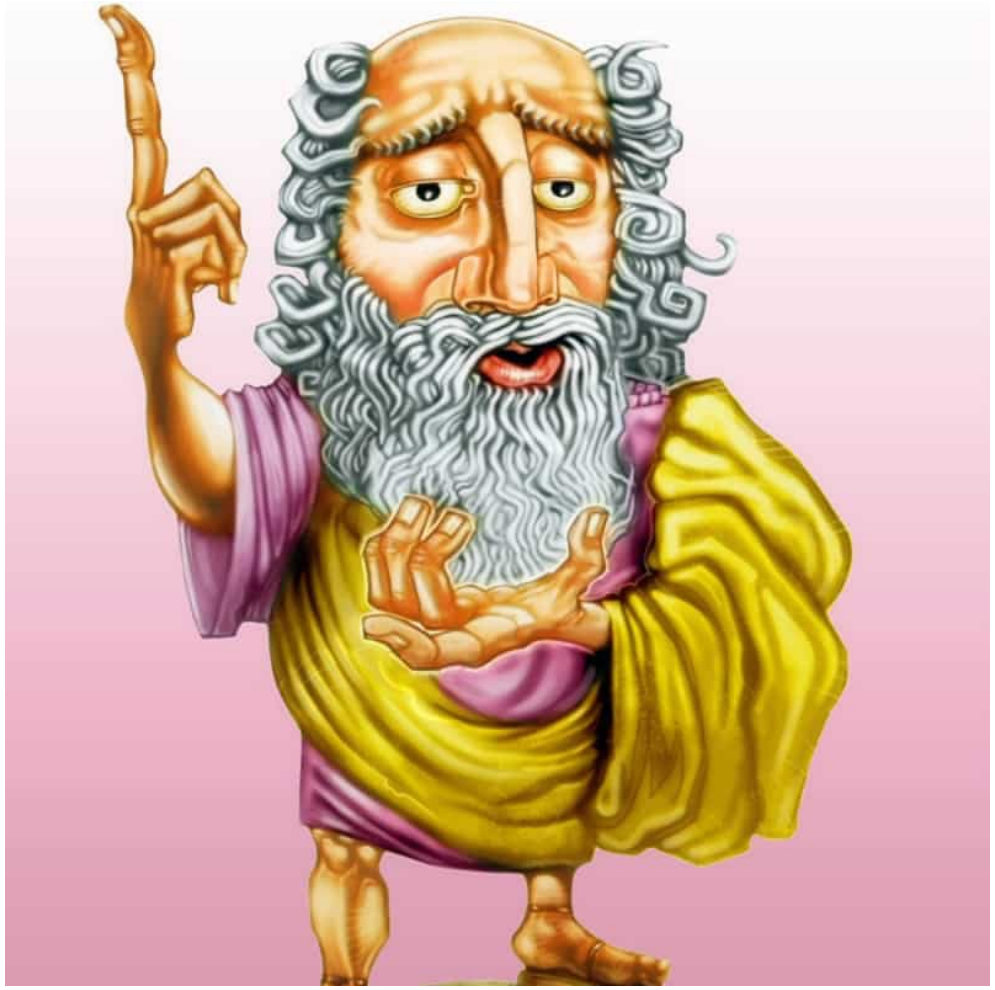
Lottery Propositions

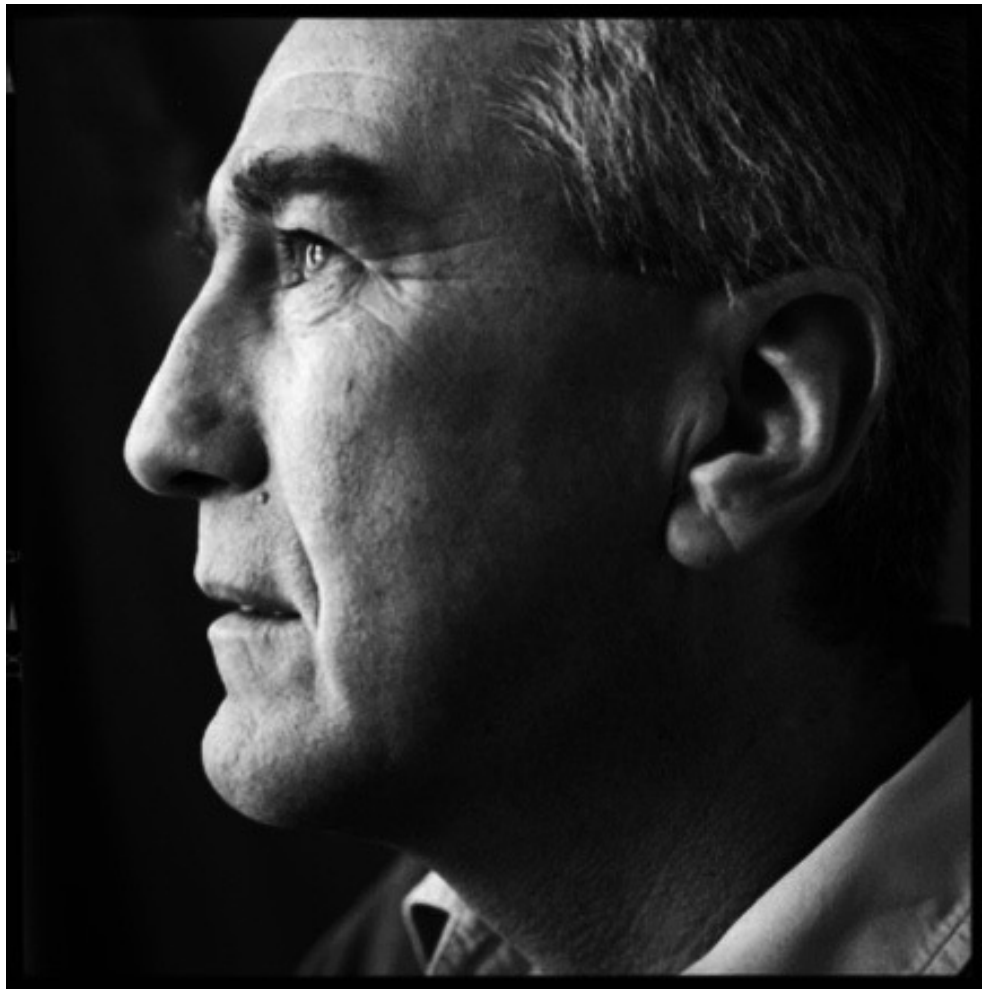
- You hold a ticket (say, #481,408) in a fair lottery.
- There are one million tickets and only one winning ticket.
- The winning number has been drawn, but you have not yet heard the result.
- Do you *know* that your ticket is *not* the winning ticket?

Why is Normic Support Valuable?

- It enhances reliability.
  - It rules out *a potential source* of error.
- It provides knowledge.

Why is Knowledge Valuable?



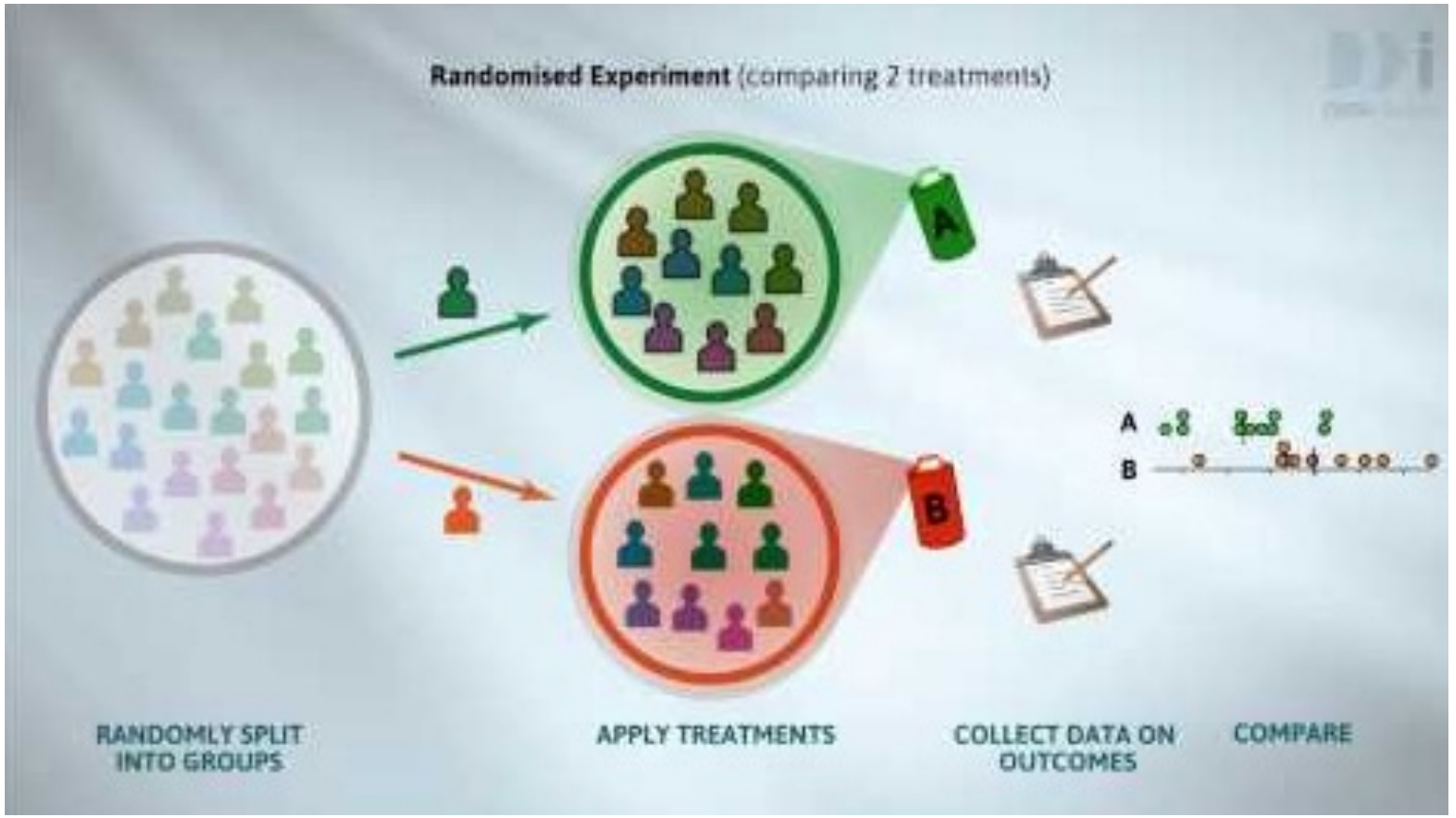


Berry on Univocality

- "*Univocality*: Concepts essentially made use of in mathematical arguments are always attended with precise necessary and sufficient defining conditions, and specific entities essentially referred to are always given precise definite descriptions."

Why is Rigor Valuable?

- It enhances reliability.
  - It rules out *a potential source* of error.

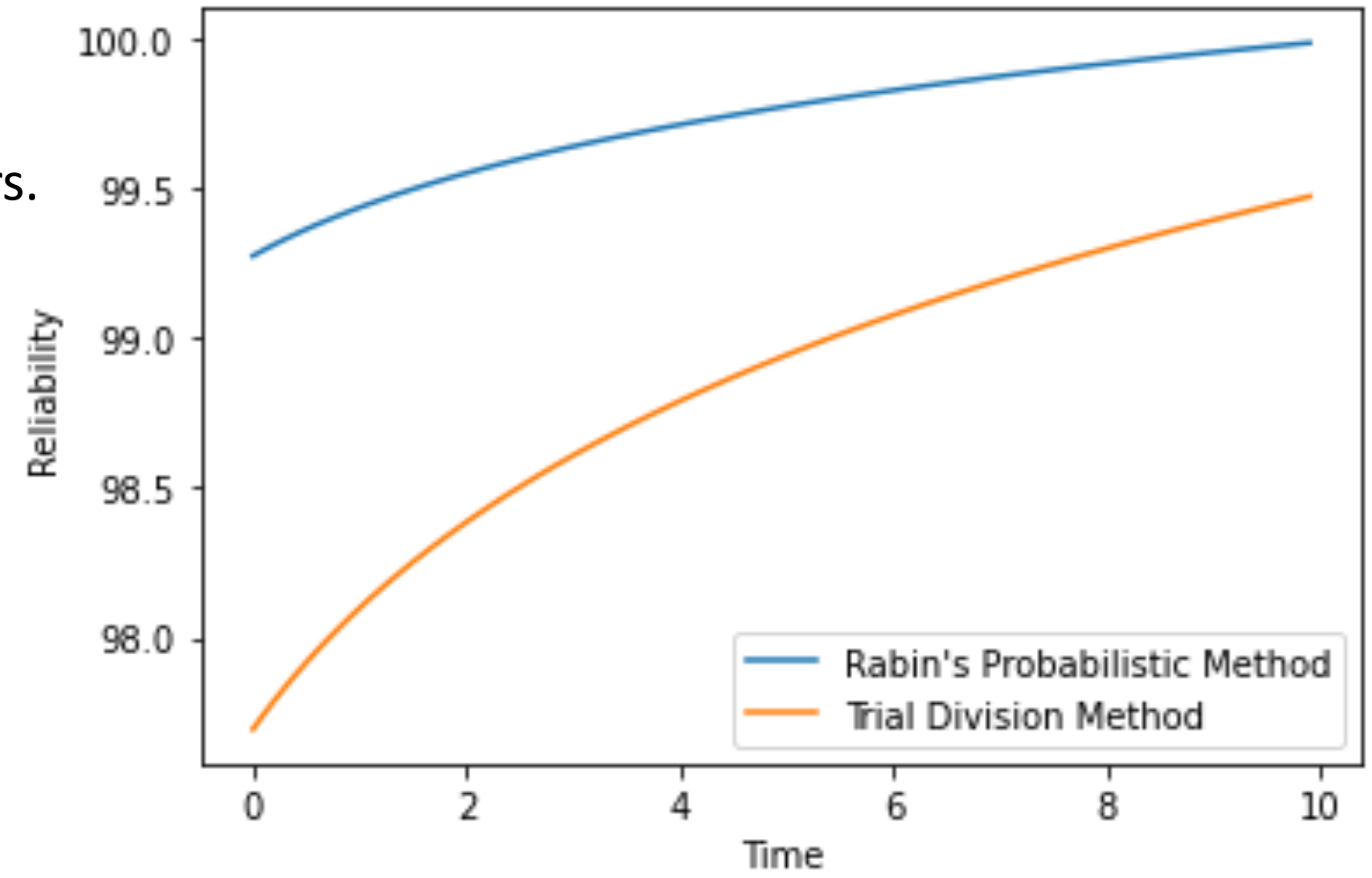


Hamami on Finite Convergence

- “Although mathematicians are fallible agents, they are also self-correcting agents. This means that when a proof is produced which only contains repairable mistakes, given enough time and energy, a mathematician or a group thereof should be able to converge towards a correct proof through a finite number of verification and correction rounds, thus providing a guarantee that the considered proposition is true, something that non-deductive reliable processes will never be able to produce”

Why is Finite Convergence Valuable?

- It enhances reliability *in the long run*.
  - It facilitates finding errors.




Extra Stuff

Truth-Tracking Account of Knowledge

- **S** knows that *p* only if …
  - **S** is likely to believe that *p* if *p* is true and …
  - **S** is unlikely to believe that *p* if *p* is false.

- My belief that "#481,408 is not the winning ticket" (based on it being a fair lottery) is *not sensitive*.
- But my belief that "66,998,713 is prime" (based on Rabin's probabilistic method) is *sensitive*.

Hamami on Lottery Propositions

- “66,998,713 is prime” is not a lottery proposition.
- But “147,377 is not a witness to the compositeness of 66,998,713” is a lottery proposition.
- And if I know that “66,998,713 is prime,” then I know that “147,377 is not a witness to the compositeness of 66,998,713.”
- So, I do not know that “66,998,713 is prime.”