What does a formal proof look like?

This document shows a small example of a formal, machine-checked proof.

The example we pick is the proof for a theorem of standard mathematics from Freek Wiedijk's compilation *The Seventeen Provers of the World* [2]. We show that the size of the diagonal of a square of side 1 is not *rational*, i.e., that it cannot be written as the division of an integer by another integer. Remember that according to Pythagoras, the size of the diagonal d of a 1 by 1 square is $\sqrt{2}$, because $d^2 = 1^2 + 1^2$.

A mathematician might phrase this theorem as follows.

Theorem 1 *$\sqrt{2}$ is irrational: there are no integers a and b such that $\sqrt{2} = \frac{a}{b}$, where the fraction $\frac{a}{b}$ is irreducible.*

A fraction is irreducible if it is in its simpliest form (e.g. 2/4 and 50/100 both represent the same irreducible fraction 1/2). An irreducible fraction $\frac{a}{b}$ is defined by the fact that a and b are *relatively prime*, or *coprime*, i.e., that there is no number diving both a and b other than 1 (denoted $gcd(a, b) = 1$, where *gcd* stands for the *greater common divisor*).

Informal proof

Several different proofs exist for this theorem. One of the easiest one is using the concept of proof by contraposition: we prove that $\sqrt{2}$ is irrational by proving that if it was rational, then we would have a contradiction.

So we first assume that $\sqrt{2}$ is rational. This means that we have two integers a and b such that $\sqrt{2} = \frac{a}{b}$, where the fraction $\frac{a}{b}$ is irreducible. We therefore have that $a^2 = 2b^2$. Now, by definition of even numbers, this gives that a^2 is even, and this implies that a itself is even (as the square of an odd number is odd). So there exists a k such that $a = 2k$. If we replace a by $2k$ in our original equation, we obtain $4k^2 = 2b^2$, which implies that $b^2 = 2k^2$, meaning that b^2, and therefore b itself are also even.

Here we reach the contradiction because we have a and b both even, which contradicts the fact that $\frac{a}{b}$ is irreducible (2 divides both a and b so $gcd(a, b) \neq 1$). Our first assumption was thus false: $\sqrt{2}$ cannot be rational.

Formal proof in Isabelle/HOL

The fully formal, machine-checked proof of the same theorem in the prover Isabelle/HOL [1] is a bit longer with more detail, but follows the same line of reasoning.

We first prove a more general lemma stating that the square root of any prime number is irrational, and use it to prove that in particular the square root of the prime number 2 is irrational.

In the machine version we write *sqrt q* for $\sqrt{q}$ and we explicitly convert between natural numbers and real number using the function *real*. The proof is a formal statement followed by a sequence of commands to the theorem prover that are phrased in such a way that they are still readable by humans (or at least human experts).

The nicely written-out proof below is due to Makarius Wenzel.

theorem *sqrt-prime-irrational*:
  assumes *prime p*
  shows *sqrt* (*real p*) $\notin \mathbb{Q}$
proof
  from ‹*prime p*› **have** *p*: $1 < p$ **by** (*simp add*: *prime-def*)
  assume *sqrt* (*real p*) $\in \mathbb{Q}$
  then obtain *m n* **where**
      n: $n \neq 0$ **and** *sqrt-rat*: $|sqrt\ (real\ p)| = real\ m\ /\ real\ n$
    and *gcd*: *gcd* (*m*, *n*) = 1 **..**
  have *eq*: $m^2 = p * n^2$
  proof −
    from *n* **and** *sqrt-rat* **have** $real\ m = |sqrt\ (real\ p)| * real\ n$ **by** *simp*
    then have $real\ (m^2) = (sqrt\ (real\ p))^2 * real\ (n^2)$
      by (*auto simp add*: *power2-eq-square*)
    also have $(sqrt\ (real\ p))^2 = real\ p$ **by** *simp*
    also have $\ldots * real\ (n^2) = real\ (p * n^2)$ **by** *simp*
    finally show *?thesis* **..**
  qed
  have *p dvd m* ∧ *p dvd n*
  proof
    from *eq* **have** *p dvd* m^2 **..**
    with ‹*prime p*› **show** *p dvd m* **by** (*rule prime-dvd-power-two*)
    then obtain *k* **where** $m = p * k$ **..**
    with *eq* **have** $p * n^2 = p^2 * k^2$ **by** (*auto simp add*: *power2-eq-square mult-ac*)
    with *p* **have** $n^2 = p * k^2$ **by** (*simp add*: *power2-eq-square*)
    then have *p dvd* n^2 **..**
    with ‹*prime p*› **show** *p dvd n* **by** (*rule prime-dvd-power-two*)
  qed
  then have *p dvd gcd* (*m*, *n*) **..**
  with *gcd* **have** *p dvd 1* **by** *simp*
  then have $p \leq 1$ **by** (*simp add*: *dvd-imp-le*)
  with *p* **show** *False* **by** *simp*
qed

corollary *sqrt* (*real* (*2*::*nat*)) $\notin \mathbb{Q}$
  by (*rule sqrt-prime-irrational*) (*rule two-is-prime*)

We are not always patient enough to explain all details to the human reader, we sometimes switch to a more machine-oriented style. It is quicker to type, but does not offer much in the way of explanation. This might be fine, though. The computer will check that the proof is right, and sometimes you only want to know what is proved, not necessarily how the proof works.

theorem *sqrt-prime-irrational*: *prime p* ⟹ *sqrt* (*real p*) $\notin \mathbb{Q}$
  apply *clarsimp*
  apply (*elim rationals-rep*)
  apply *simp*
  apply (*simp add*: *nonzero-eq-divide-eq*)
  apply (*drule arg-cong* [**where** $f = \lambda x.\ x*x$])

```
  apply (simp only: mult-ac)
  apply (simp only: power2-eq-square[symmetric])
  apply (simp only: real-sqrt-pow2)
  apply (simp only: mult-assoc[symmetric])
  apply (simp add: power2-eq-square)
  apply (simp only: real-of-nat-mult[symmetric])
  apply (simp only: real-of-nat-inject)
  apply (simp add: power2-eq-square[symmetric] eq-commute)
  apply (frule-tac m=m in prime-dvd-power-two, simp)
  apply (frule-tac m=n in prime-dvd-power-two)
   apply (frule iffD1 [OF dvd-def], clarsimp)
   apply (simp add: power2-eq-square mult-ac prime-def)
   apply (simp only: mult-assoc[symmetric])
   apply (simp add: eq-commute)
  apply (drule (1) gcd-greatest)
  apply (thin-tac p dvd n)
  apply (drule dvd-imp-le, simp)
  apply (clarsimp simp: prime-def)
done
```

References

[1] T. Nipkow, L. Paulson, and M. Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, volume 2283 of *LNCS*. Springer, 2002.

[2] F. Wiedijk, editor. *The Seventeen Provers of the World, Foreword by Dana S. Scott*, volume 3600 of *LNCS*. Springer, 2006.