Leibniz in the other direction

Introduction

Superficially, this note is about an unfamiliar proof of the familiar theorem that the square root of 2 is irrational. But the particular theorem and proof are not really the point of this note, which is to contrast traditional, intuitive problem solving with the top-down, calculational techniques pioneered by Edsger Dijkstra, Wim Feijen, and Netty van Gasteren.

* *
*

A traditional argument

Here is a traditional argument to show that $\sqrt{2}$ is irrational.

Suppose, on the contrary, that $\sqrt{2}$ can be written as a fraction m/n with m and n integer, and assume without loss of generality that m and n share no factors in common. Then we have:

$$2 \;=\; m^2/n^2$$

or equivalently:

(0) $\quad 2 * n^2 \;=\; m^2 \quad .$

So 2 divides m^2, whence it divides m. Thus we can write m as $2 * p$ for some integer p. Substituting back into (0), we get:

$$2 * n^2 \;=\; 4 * p^2 \quad ,$$

which simplifies to:

$$n^2 \;=\; 2 * p^2 \quad .$$

From this we conclude that 2 divides n^2, and thus that 2 divides n. This contradicts our original assumption that m and n have no common factors, and hence establishes that $\sqrt{2}$ is irrational, QED.

I find the above argument disappointing for three reasons. First, because of the argument by contradiction; second, because of the elliptic and unmotivated "without loss of generality"; and third, because of the unmotivated decision to show that m and n

share a factor of 2 . (We will ignore completely that perhaps the biggest "rabbit out of the hat" of all is the problem statement: why are we asking if $\sqrt{2}$ is irrational?)

* *
*

A different approach

When applying the addition algorithm or solving systems of equations in algebra, we regard the numbers and formulae as meaningless symbols and simply *calculate* the answer. It would only hurt us to try to understand these operations "intuitively" , or to carry them out in English.

In the calculational style of mathematics, we wish to apply these techniques more broadly, to logic and proofs. And why shouldn't we? Mathematics is not about its applications; at its core, mathematics is about effective, logical reasoning, the medium of which is the proof.

If our business is effective reasoning, we must first set some ground rules for what constitutes efficiency. I like the simple rule: **Do not make relevant what is irrelevant.** (In other guises: **Do not name what can be left unnamed.** , **Do not make unnecessary case distinctions.** , etc.) I acknowledge that this rule begs the question of how you can know something is irrelevant until you try it! So I will add the slight adagium: **Only try if all else fails.** .

Another "rule" is our preference for *opportunity-based simplification* , as opposed to *complification* . This is a distinction almost all mathematicians make instinctively when doing simple algebra, but oddly not when constructing proofs. For example, to prove:

$$x^2 - y^2 \;=\; (x - y) * (x + y)$$

in the following way:

$$\begin{array}{ll} & x^2 - y^2 \\ = & \quad \{ \text{ adding and subtracting } \; x * y \; \} \\ & x^2 \;+\; x * y \;-\; x * y \;-\; y^2 \\ = & \quad \{ \text{ factoring } \} \\ & x * (x + y) \;-\; y * (x + y) \\ = & \quad \{ \text{ factoring } \} \\ & (x - y) * (x + y) \end{array}$$

requires the unmotivated invention of the term $x * y$. Whereas the calculation:

$$
\begin{array}{ll}
 & (x - y) * (x + y) \\
= & \quad \{ \text{ distributive property } \} \\
 & x * (x + y) \ - \ y * (x + y) \\
= & \quad \{ \text{ distributive property } \} \\
 & x^2 \ + \ x * y \ - \ x * y \ - \ y^2 \\
= & \quad \{ \text{ cancellation } \} \\
 & x^2 - y^2
\end{array}
$$

requires no invention at all: each step is of the type "there is only one thing you can do" .

* *
*

A calculational tool

Before we return to the problem at hand, we need a calculational tool for our toolbox. Just as addition is difficult without knowing the addition algorithm, and solving systems of equations is difficult without knowing how to manipulate algebraic expressions, so is the calculational style difficult without knowing basic logical rules and general "tricks of the trade" .

Here I give one such "trick" , and you will have to take my word when I say it is completely general. It is the famous Leibniz rule: substitution of equals for equals. Usually we use this rule in strengthening chains of reasoning, as a way of eliminating function applications. The corresponding proof step is:

$$
\begin{array}{ll}
 & f.x = f.y \\
\Leftarrow & \quad \{ \text{ Leibniz } \} \\
 & x = y \qquad ,
\end{array}
$$

for any f , x , and y of the appropriate types.

(Note that I use an infix low dot "." to denote function application, writing $f.x$ for the more conventional $f(x)$. There doesn't seem to be a need for the traditional half-prefix, half-postfix notation, and with the infix dot, there is the added advantage that parentheses are used solely as syntactic delimiters.)

The contrapositive of Leibniz's rule is what we will use, in the form:

$$
\begin{array}{ll}
 & x \neq y \\
\Leftarrow & \quad \{ \text{ Zinbiel } \} \\
 & f.x \neq f.y
\end{array}
$$

Note that Leibniz used in this way requires the invention of a function f, a decidedly complifying step. Since we prefer simplification to complification, we should not use the Zinbiel rule without good reason; that is, not unless a choice for f suggests itself. As we will see, such a function will suggest itself.

So much for our methodological introduction.

* *
*

A calculational proof

Let x be of type nonnegative real. We define the square root $\sqrt{x}$ as the nonnegative solution of the following equation:

$$y: \quad y * y = x \quad .$$

So to show that $\sqrt{2}$ is irrational is to show that no rational number solves the above equation. Or in symbols, to show that for all natural m and n, with $n \neq 0$, we have:

(1) $\quad (m/n) * (m/n) \neq 2 \quad .$

We take (1) as our demonstrandum.

Because $n \neq 0$, we can simplify (1) by multiplying through by $n * n$, thereby eliminating the division operator. Thus our first proof step is as follows:

$$
\begin{array}{ll}
 & (m/n) * (m/n) \neq 2 \\
\equiv & \quad \{ \text{ algebra, using } n \neq 0 \} \\
 & m * m \neq 2 * n * n \quad .
\end{array}
$$

We now turn our attention to:

(2) $\quad m * m \neq 2 * n * n \quad .$

* *
*

Somewhere in our proof of (2) we have to use the fact that m and n are natural, otherwise we could take $m, n := \sqrt{2}, 1$. Generally speaking, about natural numbers we know really only two interesting things: first, that the set of natural numbers is well-founded, meaning we could try to prove (2) by induction; and second, that positive natural numbers are products of unique finite bags of primes, meaning we could try to exploit prime factorization in our proof of (2) .

While there may be a proof of (2) using induction, it may, because of the two variables m and n , involve a messy double induction. In any case, we would have to choose which of the two variables to induct over.

Thus, to keep things simple, we aim to exploit factorization, and observe that we can demonstrate (2) by showing that $m * m$ and $2 * n * n$ have different bags of primes in their decompositions.

(There is a little snag we have not yet discussed: If $m = 0$, it is unclear what its prime factorization would be. But if $m = 0$, then (2) is true, so we may assume $m \neq 0$ in what follows. The logic behind this argument is discussed a bit further in JAW32 .)

We try to show that the two bags of primes are different in the simplest way I can think of, namely, by ignoring what their elements are, and just showing that the bags have different numbers of elements. To this end, we introduce a function P , defined by:

$$P.x \quad = \quad \text{the number of primes in the decomposition of } \; x \qquad .$$

Now we are in good shape to exploit Leibniz, as discussed in the methodological prelude, and we continue our calculation thus:

$$\begin{array}{ll} & m * m \;\neq\; 2 * n * n \\ \Leftarrow & \quad \{ \text{ Zinbiel } \} \\ & P.(m * m) \;\neq\; P.(2 * n * n) \qquad . \end{array}$$

* * *

To continue our calculation we need some simple properties of P , and fortunately there is a lovely such property. We offer without proof:

$$(3) \qquad P.(a * b) \;=\; P.a \,+\, P.b \qquad \text{for all } \; a \; \text{ and } \; b \qquad ,$$

an obvious corollary of the definition of P .

Thus we may continue our calculation:

$$
\begin{array}{ll}
 & P.(m*m) \;\neq\; P.(2*n*n) \\
\equiv & \quad \{ \quad (3) \quad \} \\
 & P.m + P.m \quad \neq \quad P.2 + P.n + P.n \\
\equiv & \quad \{ \text{ algebra, using } \quad P.2 = 1 \quad \text{by definition } \} \\
 & 2 * P.m \quad \neq \quad 1 \;+\; 2 * P.n \qquad .
\end{array}
$$

And now the final step hits us in the face:

$$
\begin{array}{ll}
 & 2 * P.m \quad \neq \quad 1 \;+\; 2 * P.n \\
\equiv & \quad \{ \quad \text{“even } \neq \text{ odd”} \quad \} \\
 & \textbf{true} \qquad .
\end{array}
$$

Voila! Repeating the entire proof without heuristics, we have:

$$
\begin{array}{ll}
 & \text{“ } \sqrt{2} \text{ is irrational ”} \\
\equiv & \quad \{ \text{ definition of } \sqrt{\ } \text{ and ‘irrational’ } \} \\
 & (m/n) * (m/n) \;\neq\; 2 \qquad \text{for all } \quad m, n \neq 0
\end{array}
$$

and:

$$
\begin{array}{ll}
 & (m/n) * (m/n) \;\neq\; 2 \\
\equiv & \quad \{ \text{ algebra, using } \quad n \neq 0 \quad \} \\
 & m * m \;\neq\; 2 * n * n \\
\Leftarrow & \quad \{ \text{ Zinbiel } \} \\
 & P.(m * m) \;\neq\; P.(2 * n * n) \\
\equiv & \quad \{ \text{ property of } \quad P \quad \text{and algebra } \} \\
 & 2 * P.m \;\neq\; P.2 \;+\; 2 * P.n \\
\equiv & \quad \{ \quad P.2 = 1 \quad \} \\
 & 2 * P.m \;\neq\; 1 \;+\; 2 * P.n \\
\equiv & \quad \{ \quad \text{“even } \neq \text{ odd”} \quad \} \\
 & \textbf{true} \qquad .
\end{array}
$$

Note that the only invention in this proof is P, which, far from being unmotivated, was suggested by the fact that we are working with natural numbers, and by our pursuit of simplicity.

Note also that the entire proof hinges only on property (3) of P and the fact that $P.2$ is odd. Thus with only minor modifications to the above proof, we can draw the stronger conclusion:

$\sqrt{k}$ is irrational for all k having an odd number of primes in its decomposition.

A strong theorem is the reward for a simple proof!

* *
*

Finally, let us return for a moment to our invention of P. We chose there not to take into account the nature of the elements of the bags of primes in the decompositions of $m * m$ and $2 * n * n$, and to simply count the number of primes. Now let us see what happens if we become a little more sophisticated and take something into account.

There is really only one sensible idea, given the shape of the formulae: the expression $m * m$ has no 2, while $2 * n * n$ does. Thus it makes sense to show that $m * m$ and $2 * n * n$ have different numbers of 2s in their prime decompositions. To this end, let us define:

$T.x$ = the number of 2s in the decomposition of x.

Then the above proof is valid if we replace P by T, since (3) holds for T, and since $T.2$ is odd.

This observation shows that there was some room for us to be a little less naive in our construction of the first proof, but in fact it shows more. Replacing 2 by any prime in the definition of T still preserves property (3), and hence with a little work —left to the reader— we obtain the stronger:

$\sqrt{k}$ is irrational for all k having an odd number of some prime in its decomposition.

References

Roland Backhouse "Program Construction", John Wiley and Sons, 2003, pages 37–39

Culver City, 16–17 September 2004 / Revised: NYC, 25 December 2010

Jeremy Weissmann
jeremy@mathmeth.com