Recycling proofs

Petrucio Viana*
IME–UFF

3rd World Logic Day

January 14, 2021

* Joint work with: Márcia R. Cerioli (COPPE-IM-UFRJ) & Raphael de Marreiros

Sumary

1. Natural radical numbers
2. The even-odd proof
3. The prime number proof
4. Interating the prime number proof
5. Non-conclusions

1. Natural radical numbers

Natural radical numbers

Let $r \in \mathbb{R}$

We say that r is a *natural radical number* if there are $n, a \in \mathbb{N}$ such that

$$r = \sqrt[n]{a}$$

When is a natural radical number an irrational number?

Very well known answer

$r = \sqrt[n]{a}$ is irrational iff there is no b such that $a = b^n$

Radical numbers

We are not interested in the result, but in the proofs

How to prove this fact?

More specifically, we are interested in the way we can **produce** and **write** a proof

How to produce and write a prof of this fact?

Oldest example

Let us start with the classical result:

$\sqrt{2} \notin \mathbb{Q}$

First, we examine the **even-odd proof**

Notation

We adopt the following abbreviations:

Σ	for	Suppose that ...
Δ	for	From this, we have ...
Ω	for	We know that ...
$\rightarrow\leftarrow$	for	This contradicts the hypothesis $\mathrm{MDC}(a, b) = 1$

2. The even-odd prof

Oldest example

$\sqrt{2} \notin \mathbb{Q}$

Proof by *Reductio ad Absurdum*:

$$\Sigma : \sqrt{2} = a/b \wedge \mathrm{MCD}(a, b) = 1$$

$$\Delta : 2b^2 = a^2$$

$$\Delta : a^2 \in 2\mathbb{N}$$

$$\Omega : a \in 2\mathbb{N} \vee a \in 2\mathbb{N} + 1$$

$$\Sigma : a \in 2\mathbb{N} + 1$$

$$\Delta : a = 2n + 1$$

$$\Delta : a^2 = 4n^2 + 4n + 1$$

$$\Delta : a^2 \in 2\mathbb{N} + 1, \rightarrow\leftarrow$$

$$\Delta : a = 2m$$

Oldest example

$\sqrt{2} \notin \mathbb{Q}$

Proof by *Reductio ad Absurdum*:

$$\Sigma : \sqrt{2} = a/b \wedge \mathrm{MCD}(a,b) = 1$$

$$\Delta : 2b^2 = a^2$$

$$\Delta : a^2 \in 2\mathbb{N}$$

$$\Omega : a \in 2\mathbb{N} \vee a \in 2\mathbb{N}+1$$

$$\Sigma : a \in 2\mathbb{N}+1, \rightarrow\leftarrow$$

$$\Delta : a = 2m$$

$$\Delta : 2b^2 = 4m^2$$

$$\Delta : b^2 \in 2\mathbb{N}$$

$$\Delta : b = 2k$$

$$\Delta : \mathrm{MCD}(a,b) \geq 2 > 1, \rightarrow\leftarrow$$

What about $\sqrt{3}$?

$\sqrt{3} \notin \mathbb{Q}$

Proof by *Reductio ad Absurdum*:

$$\Sigma : \sqrt{3} = a/b \wedge \mathrm{MCD}(a, b) = 1$$

$$\Delta : 3b^2 = a^2$$

$$\Delta : a^2 \in 3\mathbb{N}$$

$$\Omega : a \in 3\mathbb{N} \vee a \in 3\mathbb{N} + 1 \vee a \in 3\mathbb{N} + 2$$

$$\Sigma : a \in 3\mathbb{N} + 1$$

$$\Delta : a = 3n + 1$$

$$\Delta : a^2 = 9n^2 + 6n + 1$$

$$\Delta : a^2 \in 3\mathbb{N} + 1, \rightarrow\leftarrow$$

What about $\sqrt{3}$?

$\sqrt{3} \notin \mathbb{Q}$

Proof by *Reductio ad Absurdum*:

$$\Sigma : \sqrt{3} = a/b \wedge \mathrm{MCD}(a, b) = 1$$

$$\Delta : 3b^2 = a^2$$

$$\Delta : a^2 \in 3\mathbb{N}$$

$$\Omega : a \in 3\mathbb{N} \vee a \in 3\mathbb{N} + 1 \vee a \in 3\mathbb{N} + 2$$

$$\Sigma : a \in 3\mathbb{N} + 1, \rightarrow\leftarrow$$

$$\Sigma : a \in 3\mathbb{N} + 2$$

$$\Delta : a = 3n + 2$$

$$\Delta : a^2 = 9n^2 + 12n + 3 + 1$$

$$\Delta : a^2 \in 3\mathbb{N} + 1, \rightarrow\leftarrow$$

What about $\sqrt{3}$?

$\sqrt{3} \notin \mathbb{Q}$

Proof by *Reductio ad Absurdum*:

$$\Sigma : \sqrt{3} = a/b \wedge \mathrm{MCD}(a, b) = 1$$

$$\Delta : 3b^2 = a^2$$

$$\Delta : a^2 \in 3\mathbb{N}$$

$$\Omega : a \in 3\mathbb{N} \vee a \in 3\mathbb{N} + 1 \vee a \in 3\mathbb{N} + 2$$

$$\Sigma : a \in 3\mathbb{N} + 1, \rightarrow\leftarrow$$

$$\Sigma : a \in 3\mathbb{N} + 2, \rightarrow\leftarrow$$

$$\Delta : a = 3m$$

$$\Delta : 3b^2 = 9m^2$$

$$\Delta : b^2 \in 3\mathbb{N}$$

$$\Delta : b = 3k$$

$$\Delta : \mathrm{MCD}(a, b) \geq 3 > 1, \rightarrow\leftarrow$$

What about $\sqrt{5}$?

$\sqrt{5} \notin \mathbb{Q}$

Proof by *Reductio ad Absurdum*:

$$\Sigma : \sqrt{5} = a/b \wedge \mathrm{MCD}(a, b) = 1$$

$$\Delta : 5b^2 = a^2$$

$$\Delta : a^2 \in 5\mathbb{N}$$

$$\Omega : a \in 5\mathbb{N} \vee a \in 5\mathbb{N} + 1 \vee \cdots \vee a \in 5\mathbb{N} + 4$$

$$\Sigma : a \in 5\mathbb{N} + 1, \rightarrow\leftarrow$$

$$\vdots$$

$$\Sigma : a \in 5\mathbb{N} + 4, \rightarrow\leftarrow$$

$$\Delta : a \in 5\mathbb{N}$$

$$\Delta : b^2 \in 5\mathbb{N}$$

$$\Delta : b \in 5\mathbb{N}$$

$$\Delta : \mathrm{MCD}(a, b) \geq 5 > 1, \rightarrow\leftarrow$$

We already know what to do!

p is prime $\Rightarrow \sqrt{p} \notin \mathbb{Q}$

Proof by *Reductio ad Absurdum*:

$$\Sigma : \sqrt{p} = a/b \wedge \mathrm{MCD}(a,b) = 1$$

$$\Delta : pb^2 = a^2$$

$$\Delta : a^2 \in p\mathbb{N}$$

$$\Omega : a \in p\mathbb{N} \vee a \in p\mathbb{N} + 1 \vee \cdots \vee a \in p\mathbb{N} + (p-1)$$

$$\Sigma : a \in p\mathbb{N} + 1, \rightarrow\leftarrow$$

$$\vdots$$

$$\Sigma : a \in p\mathbb{N} + (p-1), \rightarrow\leftarrow$$

$$\Delta : a \in p\mathbb{N}$$

$$\Delta : pb^2 = p^2 m^2$$

$$\Delta : b^2 \in p\mathbb{N}$$

$$\Delta : b \in p\mathbb{N}$$

$$\Delta : \mathrm{MCD}(a,b) \geq p > 1, \rightarrow\leftarrow$$

But the problem is ...

For each prime number p, we have a proof that $\sqrt{p} \notin \mathbb{Q}$, whose length increase when p increase

If $p = 282,589,933 - 1$ which has $24,862,048$ digits the proof would take more than 10.000 pages

But the problem is . . .

To recycle the proof, we need to write, case by case, that all the statements

$$a \in p\mathbb{N} + 1, \dots, a \in p\mathbb{N} + (p - 1)$$

are contradictory

The question is:

Can these local proofs (one for each fixed prime number) merge into a proof for the general case (an arbitrary prime number)?

I mean, proofs having approximately the same length

3. The prime number proof

Prime numbers

A point that deserves to be highlighted is that in the odd-even proofs, we do not explicitly write the part of the proof where the hypothesis "p is prime " is used

What is a prime number?

Let $p \in \mathbb{N}$, $p \neq 0, 1$

p is *baby-prime* if $\forall a \in \mathbb{N} : a < p \Rightarrow \neg(a \mid p)$

p is *teenage-prime* if $\forall a \in \mathbb{N} : a \mid p \Rightarrow a = 1 \vee a = p$

p is *adult-prime* if $\forall a, b \in \mathbb{N} : p \mid ab \Rightarrow p \mid a \vee p \mid b$

Prime numbers

We experimented with the notions of baby-prime and teenage-prime numbers and were only able to produce proofs that increase when the prime number increases

On the other hand, the notion of adult-prime gives us the **prime number proof**

$\sqrt{2} \notin \mathbb{Q}$

Proof by Reductio ad Absurdum:

$$\Sigma : \sqrt{2} = a/b \wedge \mathrm{MDC}(a, b) = 1$$

$$\Delta : 2b^2 = a^2$$

$$\Delta : 2 \mid a^2$$

$$\Omega : 2 \text{ is adult-prime}$$

$$\Delta : 2 \mid a$$

$$\Delta : a = 2m$$

$$\Delta : 2b^2 = 4m^2$$

$$\Delta : b^2 = 2m^2$$

$$\Delta : 2 \mid b^2$$

$$\Omega : 2 \text{ is adult-prime}$$

$$\Delta : 2 \mid b$$

$$\Delta : \mathrm{MCD}(a, b) \geq 2 > 1, \rightarrow\leftarrow$$

$\sqrt{3} \notin \mathbb{Q}$

Proof by Reductio ad Absurdum:

$$\Sigma : \sqrt{3} = a/b \wedge \mathrm{MDC}(a, b) = 1$$

$$\Delta : 3b^2 = a^2$$

$$\Delta : 3 \mid a^2$$

$$\Omega : 3 \text{ is adult-prime}$$

$$\Delta : 3 \mid a$$

$$\Delta : a = 3m$$

$$\Delta : 3b^2 = 9m^2$$

$$\Delta : b^2 = 3m^2$$

$$\Delta : 3 \mid b^2$$

$$\Omega : 3 \text{ is adult-prime}$$

$$\Delta : 3 \mid b$$

$$\Delta : \mathrm{MCD}(a, b) \geq 3 > 1, \rightarrow\leftarrow$$

p is adult-prime $\Rightarrow \sqrt{p} \notin \mathbb{Q}$

Proof by Reductio ad Absurdum:

$$\Sigma : \sqrt{p} = a/b \wedge \mathrm{MDC}(a,b) = 1$$

$$\Delta : pb^2 = a^2$$

$$\Delta : p \mid a^2$$

$$\Omega : p \text{ is adult-prime}$$

$$\Delta : p \mid a$$

$$\Delta : a = pm$$

$$\Delta : pb^2 = p^2 m^2$$

$$\Delta : b^2 = pm^2$$

$$\Delta : p \mid b^2$$

$$\Omega : p \text{ is adult-prime}$$

$$\Delta : p \mid b$$

$$\Delta : \mathrm{MCD}(a,b) \geq p > 1, \rightarrow\leftarrow$$

The main point in the proofs above is . . .

We had not merged (or tried to merge) a series of local proofs (one for each fixed prime number) in a proof for the general case (an arbitrary prime number)

In this case, **exactly the same proof** took care of all cases!!!

All the proofs have the same length!!!

4. Iterating prime number proof

The main question

We proved that $\sqrt{2} \notin \mathbb{N}$ (using the notion of an adult-prime)

After that we showed that the same proof shows that $\sqrt{3} \notin \mathbb{N}$

After that we showed that the same proof shows that $\sqrt{p} \notin \mathbb{N}$, for any prime number p

How far we can go with the prime number proof?

sketches for a solution

Let $r \in \mathbb{R}$

We say that r is **suitable for the prime number proof** if (a version of) the prime number proof shows that $r \notin \mathbb{Q}$

We proved that $\sqrt{p}$ is suitable for the prime number proof, for every prime number p

Starting a solution

Now we exhibit some numbers which are also suitable for the prime number proof

More specifically, we treat the numbers of the forms $\sqrt[n]{p^m}$, considering the cases:

1. $m = 1$ and $n = 2$
2. $n > m \geq 2$
3. $(l + 1)n > m > ln \geq 2$, for $l = 1, 2, 3, 4, \ldots$

$n \geq 2 \Rightarrow \sqrt[n]{p}$ is suitable for the prime number proof

Proof by Reductio ad Absurdum:

$$
\begin{array}{ll}
\Sigma & : n \geq 2 \wedge \sqrt[n]{p} = a/b \wedge \mathrm{MDC}(a, b) = 1 \\
\Delta & : pb^n = a^n \\
\Delta & : p \mid a^n \\
\Omega & : p \text{ is adult-prime} \\
\Delta & : p \mid a \\
\Delta & : a = pm \\
\Delta & : pb^n = p^n m^n \\
\Delta^{-7} & : p^{n-1} \in \mathbb{N} \\
\Delta & : b^n = p^{n-1} m^n \\
\Delta & : p \mid b^n \\
\Omega & : p \text{ is adult-prime} \\
\Delta & : p \mid b \\
\Delta & : \mathrm{MCD}(a, b) \geq p > 1, \rightarrow\leftarrow
\end{array}
$$

$n > m \geq 2 \Rightarrow \sqrt[n]{p^m}$ is suitable for the prime number proof

Proof by Reductio ad Absurdum:

$$
\begin{array}{ll}
\Sigma & : n > m \geq 2 \wedge \sqrt[n]{p^m} = a/b \wedge \mathrm{MDC}(a,b) = 1 \\
\Delta & : p^m b^n = a^n \\
\Delta & : p^m \mid a^n \\
\Omega & : p \text{ is adult-prime} \\
\Delta & : p \mid a \\
\Delta & : a = pm \\
\Delta & : p^m b^n = p^n m^n \\
\Delta^{-7} & : p^{n-m} \in \mathbb{N} \\
\Delta & : b^n = p^{n-m} m^n \\
\Delta & : p \mid b^n \\
\Omega & : p \text{ is adult-prime} \\
\Delta & : p \mid b \\
\Delta & : \mathrm{MCD}(a,b) \geq p > 1, \rightarrow\leftarrow
\end{array}
$$

Continuing a solution

Now, to move from

$$n > m \geq 2 \text{ and } p \text{ is prime} \Rightarrow \sqrt[n]{p^m} \notin \mathbb{Q}$$

to

$$m > n \geq 2 \Rightarrow \sqrt[n]{p^m} \notin \mathbb{Q}$$

we need interate the core of the reasoning employed in the prime number proof

If $m = nk$ we have $\sqrt[n]{p^m} = p^k \in \mathbb{Q}$

So, we analyse the cases when m is between two consecutive multiples of n, that is, $(l+1)n > m > ln$, for $l = 1, 2, 3, 4, \ldots$

$2n > m > n \geq 2 \Rightarrow \sqrt[n]{p^m} \notin \mathbb{Q}$

Proof by Reductio ad Absurdum:

$$
\begin{array}{ll}
\Sigma & : 2n > m > n \geq 2 \wedge \sqrt[n]{p^m} = a/b \wedge \mathrm{MDC}(a,b) = 1 \\
\Delta & : p^m b^n = a^n \\
\Delta & : p^m \mid a^n \\
\Omega & : p \text{ is adult-prime} \\
\Delta & : p \mid a \\
\Delta & : a = pm \\
\Delta & : p^m b^n = p^n m^n \\
\Delta^{-7} & : p^{m-n} \in \mathbb{N} \\
\Delta & : p^{m-n} b^n = m^n \\
\Delta^{-6} & : p \mid m \\
\Delta & : m = pk
\end{array}
$$

Continues on the next page . . .

$2n > m > n \geq 2 \Rightarrow \sqrt[n]{p^m} \notin \mathbb{Q}$

Continuing the previous page . . .

$$
\begin{aligned}
\Delta^{-3} &: p^{m-n}b^n = p^n k^n \\
\Delta^{-12} &: p^{2n-m} \in \mathbb{N} \\
\Delta^{-2} &: b^n = p^{2n-m}k^n \\
\Omega &: p \text{ is adult-prime} \\
\Delta &: p \mid b \\
\Delta &: \mathrm{MCD}(a,b) \geq p, \rightarrow\leftarrow
\end{aligned}
$$

$3n > m > 2n \geq 2 \Rightarrow \sqrt[n]{p^m} \notin \mathbb{Q}$

Proof by Reductio ad Absurdum:

$$
\begin{aligned}
\Sigma &: 3n > m > 2n \geq 2 \wedge \sqrt[n]{p^m} = a/b \wedge \mathrm{MDC}(a,b) = 1 \\
\Delta &: p^m b^n = a^n \\
\Delta &: p^m \mid a^n \\
\Omega &: p \text{ is adult-prime} \\
\Delta &: p \mid a \\
\Delta &: a = pm \\
\Delta &: p^m b^n = p^n m^n \\
\Delta^{-7} &: p^{m-n} \in \mathbb{N} \\
\Delta &: p^{m-n} b^n = m^n \\
\Delta^{-6} &: p \mid m \\
\Delta &: m = pk
\end{aligned}
$$

Continues on the next page . . .

$3n > m > 2n \geq 2 \Rightarrow \sqrt[n]{p^m} \notin \mathbb{Q}$

Continuing the previous page ...

$$
\begin{aligned}
&\Delta^{-3} &&: p^{m-n} b^n = p^n k^n \\
&\Delta^{-12} &&: p^{m-2n} \in \mathbb{N} \\
&\Delta^{-2} &&: p^{m-2n} b^n = k^n \\
&\Omega &&: p \text{ is adult-prime} \\
&\Delta &&: p \mid k \\
&\Delta &&: k = pl \\
&\Delta^{-4} &&: p^{m-2n} b^n = p^n l^n \\
&\Delta^{-19} &&: p^{3n-m} \in \mathbb{N} \\
&\Delta^{-2} &&: b^n = p^{3n-m} l^n \\
&\Omega &&: p \text{ is adult-prime} \\
&\Delta &&: p \mid b \\
&\Delta &&: \mathrm{MCD}(a,b) \geq p, \rightarrow\leftarrow
\end{aligned}
$$

Going on

Using the same approach we can obtain a prime number like proof of

$$4n > m > 3n \geq 2 \Rightarrow \sqrt[n]{p^m}$$

by three iterations of the argument.

Also a prime number like proof of

$$5n > m > 4n \geq 2 \Rightarrow \sqrt[n]{p^m}$$

by four iterations of the same argument.

Going on

Is it possible to merge all these proofs in a unique proof of

$$(l+1)n > m > ln \geq 2 \Rightarrow \sqrt[n]{p^m}$$

by l iterations of the argument?

For iterate the passage from $p \mid a$ to $p \mid b$, we need the following:

Lemma: If $m, n, p, a, b \in \mathbb{N}$, $n \geq 2$ and p is prime, then $\forall l \in \mathbb{N}$, if $m > ln$ e $p^m b^n = a^n$, $\exists k \in \mathbb{N}$ such that $p^{m-kn} b^n = p^n k^n$.

The proof goes by induction on l.

$(l+1)n > m > ln \geq 2 \Rightarrow \sqrt[n]{p^m} \notin \mathbb{Q}$

Proof by Reductio ad Absurdum:

$$\begin{aligned}
\Sigma &: (l+1)n > m > ln \geq 2 \wedge \sqrt[n]{p^m} = a/b \wedge \mathrm{MDC}(a,b) = 1 \\
\Delta &: p^m b^n = a^n \\
\Delta &: p^m \mid a^n \\
\Omega &: p \text{ is adult-prime} \\
\Delta &: p \mid a \\
\Delta^{-4}, \text{Lemma} &: p^{m-ln} b^n = p^n k^n \\
\Delta^{-6} &: p^{(l+1)n-m} \in \mathbb{N} \\
\Delta &: b^n = p^{(l+1)n-m} k^n \\
\Delta &: p \mid b \\
\Delta &: \mathrm{MCD}(a,b) \geq p, \rightarrow\leftarrow
\end{aligned}$$

5. Non-conclusions

Proofs of the irrationality of $\sqrt{2}$

There are many proofs of the irrationality of $\sqrt{2}$

The even-odd proof seems to be applicable, case-by-case, only to numbers of the form $\sqrt{p}$

The prime number proof is applicable to all numbers of the form $\sqrt[n]{p^m}$.

We already know that is also applicable to all numbers of the form $\sqrt[n_1]{p}_1 \cdots \sqrt[n_k]{p}_k$

Proofs of the irrationality of $\sqrt{2}$

What about the numbers of the form $\sqrt[n_1]{p_1^{m_1}}\sqrt[n_2]{p_2^{m_2}}\cdots\sqrt[n_k]{p_k^{m_k}}$?

So, we have this concept of a class of radical numbers for which a proof of the irrationality of $\sqrt{2}$ applies

We are developing this idea in order to get some answer to the following question

A not precise question

Given a proof showing that $\sqrt{2}$ is irrational, how far can we repeat (or iterate) the reasoning used in the proof to prove that a number is irrational?

In other words, which is the biggest set of numbers that “the idea used in the proof” shows are irrational?