Rigor in Mathematics

James Guo

January 3rd, 2024

During mathematics classes in high school, many things are "kind of" taken for granted. At most times, you are "given" a more intuitive explanation without a rigorous proof. In many high school math problems, you are fine, but if you dive into many cases in college-level mathematics, it must be treated better.

0.1. Example: Define a function $f : (0, 1) \to \mathbb{R}$ as follows:

$$f(x) = \begin{cases} 0, & \text{if } x \text{ is irrational,} \\ \frac{1}{n}, & \text{if } x = \frac{m}{n}, \text{ where } m, n \in \mathbb{Z}^+ \text{ and } \gcd(m, n) = 1. \end{cases}$$

(a) Determine if f is continuous at irrational points, and if f is continuous at rational points.

(b) (If one has learned Calculus.) Determine if f is differentiable at irrational points.

Clearly, the definition of "continuity" in *Honors Integrated Math II* is too intuitive for this case, and it fails to account when the function f is defined obscurely. Even you learned high school *Calculus*, you can hardly get to a conclusion of differentiability without the ϵ-δ definition of continuity.

0.2. Example: Note that *countable* is defined for a set when you can number each element in the set to a natural number (that is $\mathbb{N}$). Clearly, by this definition, we know that integers (that is $\mathbb{Z}$) are countable, since we can establish the following function $f : \mathbb{Z} \to \mathbb{N}$ so every number can be mapped:

$$f(x) = \begin{cases} 2x, & \text{if } x \geq 0, \\ -2x - 1, & \text{if } x < 0. \end{cases}$$

Therefore, a set could be countable even if it is infinite. Then consider the following two sets of infinite elements.

(a) Determine if $\mathbb{Q}$ is countable?

(b) Determine if $\mathbb{R}$ is countable?

With such examples, our intuition might really relate *sets cardinality* (how much elements) with countability, which is not the real case. Therefore, learning in mathematics would require higher rigor, and, in fact, many seemingly right conclusions might be incorrect on some special cases (called *contradictions*).

Hopefully, the above examples should convince you that many mathematics requires more rigor. For the sake of this talk, I will bring back a very "intuitive" question that you definitely have learned in *Honors Integrated Math II* (hopefully in regular or accelerated version as well, but I cannot verify that).

1.1. Problem: Fix $a > 1$, and let x and y be real numbers, show that:

$$a^x \cdot a^y = a^{x+y}.$$

Hopefully, your instructors should have told you that this is true. Further, one shall also hope that this holds, else many developed theories and calculations based on this results must be wrong. However, we are back to our question, how can we show that our intuition is correct?

The good news is that this "conjecture" is trivially correct for all x and y being natural numbers. You can easily found it holding by applying the definition of exponentials as *multiplying things together*, that is:

$$a^x \cdot a^y = \underbrace{a \cdot a \cdot \cdots \cdot a}_{x \text{ times}} \cdot \underbrace{a \cdot a \cdot \cdots \cdot a}_{y \text{ times}} = \underbrace{a \cdot a \cdot \cdots \cdot a}_{x+y \text{ times}} = a^{x+y}.$$

Diligent readers shall already realize how we can extend the proof for all integer, namely consider that a^{-x} being the *reciprocal* of the number and the proof shall get through.

Now, we shall push this forward to rational numbers and then real numbers, and you might found lost. Here, you would be provided with a theorem so we could get forward.

1.2. Theorem: For every real $x > 0$ and every integer $n > 0$, there exists a unique positive $y \in \mathbb{R}$ such that $y^n = x$.

The proof of this theorem would requires proof for both *existence* and *uniqueness* of y. This proof is left as an exercise to capable readers (cf. Exercise 3).

1.3. Lemma: The case for **Problem 1.1** holds for all x and y being rational numbers.

To prove this lemma, we first want to establish that for all rational x, we can write $a^x = (a^p)^{1/q}$ where p and q are integers.

Therefore, we let $r = m/n = p/q$, so we have:

$$rnq = mq = np.$$

Then, let $y_1 = (a^m)^{1/n}$ and $y_2 = (a^p)^{1/q}$, we have:

$$y_1^{rnq} = y_1^n p = ((a^m)^{1/n})^{np} = a^{mp} \text{ and } y_2^{rnq} = y_2^m q = ((a^p)^{1/q})^{mq} = a^{mp}.$$

Therefore, by knowing that $y_1^{rnq} = a^{mp} = y_2^{rnq}$, and based on **Theorem 1.2**, we know that:

$$y_1 = y_2 \Longrightarrow (a^m)^{1/n} = (a^p)^{1/q}.$$

Therefore, we know that for all rational x, we can write $a^x = (a^p)^{1/q}$ where p and q are integers.

Then, let $x = \frac{\alpha}{\beta}$ and $y = \frac{\gamma}{\delta}$, where $\alpha, \gamma \in \mathbb{Z}$ and $\beta, \delta \in \mathbb{Z}^+$. There, we can rewrite the expression as:

$$a^{x+y} = a^{\frac{\alpha}{\beta} + \frac{\gamma}{\delta}} = a^{\frac{\alpha\delta + \beta\gamma}{\beta\delta}} = (a^{\alpha\delta + \beta\gamma})^{1/(\beta\delta)}.$$

By definition of exponents, we have:

$$a^{x+y} = (a^{\alpha\delta} a^{\beta\gamma})^{1/(\beta\delta)}.$$

Here, we want to break $a^{\alpha\delta} a^{\beta\gamma}$ apart, so we want to show that for $a, b \in \mathbb{R}^+$ and $n \in \mathbb{Z}^+$ that $(ab)^{1/n} = a^{1/n} b^{1/n}$. Here, we notice that:

$$(a^{1/n} b^{1/n})^n = a^{n/n} b^{n/n} = ab,$$

then, by **Theorem 1.2** again, there exists a single positive $(a^{1/n}b^{1/n})^{n/n} = a^{1/n}b^{1/n}$ equivalent to $(ab)^{1/n}$.

Therefore, we continue with the lemma (with $a^{\alpha\delta}, a^{\beta\gamma} \in \mathbb{R}^+$ and $\beta\delta \in \mathbb{Z}^+$) that:

$$a^{r+s} = (a^{\alpha\delta}b^{\beta\gamma})^{1/(\beta\delta)} = a^{(\alpha\delta)/(\beta\delta)}a^{(\beta\gamma)/(\beta\delta)} = a^{\alpha/\beta}a^{\gamma/\delta} = a^x \cdot a^y,$$

as desired. Hence, we have completed the proof for **Lemma 1.3**, which extends the validity to all rational numbers.

Given the time constraints, the rest of the proof are left to the readers (cf. Exercise 5).

Overall, mathematics is a very rigorous subject, and it is fair for you to start asking **why** for many questions. There could be some problems that come out to be too narrow, and there would be many generalizations in college to what you have seen here at high school.

In fact, this whole problem is modified and obtained from "Baby Rudin" (or *Principles of Mathematical Analysis*), which is a text for a college analysis course, and clearly one can notice that learning analysis really requires minimal math background, but more of rigor in the subject. It would be a good choice for you to explore more into mathematics if you found yourself interested in topics like this.

Exercises:

1. If you have not done so, complete **Example 0.1** and **Example 0.2**.

2. Let S be an ordered set. Suppose that $E \subseteq S$ and E is bounded above. Also suppose that there exists an $\alpha \in S$ such that:

   - α is an upper bound for E, and
   - If $\gamma < \alpha$,then γ is not an upper bound for E.

   Here, α is the **supremum** of E, written as $\alpha := \sup E$.
   Given this definition, let $E := \left\{-\frac{1}{n} \;\middle|\; n \in \mathbb{Z}^+\right\} \subsetneq \mathbb{R}$, find $\sup E$.

3. Prove **Theorem 1.2** using the definition of *supremum*. Note that you need to consider both *existence* and *uniqueness*.

4. There always exists some rational numbers between any two irrationals, to show this, follow the below instructions.

   (a) Show that if $x, y \in \mathbb{R}$ and $x > 0$, then there exists an $n \in \mathbb{Z}^+$ such that $nx > y$. This is known as the Archimedean property.

   (b) If $x, y \in \mathbb{R}$ and $x < y$, then there is a $p \in \mathbb{Q}$ such that $x < p < y$.

5. Prove **Problem 1.1** for all $x, y \in \mathbb{R}$.
   Hint: You might want to establish $a^x = \sup A(x)$ where $A(x)$ is the set of all numbers a^t such that $t \leq x$. Then, you want to show that $a^x a^y \leq a^{x+y}$ and $a^x a^y \geq a^{x+y}$ to verify that $a^x a^y = a^{x+y}$.