

Objectionable to the Intuitionists

The intuitionists will not automatically allow that for any statement Q , either Q is true or $\sim Q$ is true. Here are a few examples of statements whose usual proofs use this principle, together with the intuitionists' probable take on them. In most cases, Q is of form $(\exists x)P(x)$. If $\sim Q$ is false, does it follow that Q is true?

Example 1. If $f: [a, b] \rightarrow \mathbf{R}$ is continuous, then $(\exists c \in [a, b])(f(c) = \text{lub}\{f(x): x \in [a, b]\})$.

The proof of this existence theorem does not show how to find or construct c ; rather, it derives a contradiction from the assumption that there is no such c . The intuitionists do not accept this proof, and they have discovered no intuitionistic proof with which to replace it; so for them this is not a theorem.

Example 2. Let $p \in \mathbf{N}$, $p \geq 2$. Suppose, for some $a \in \mathbf{N}$, we have discovered that $a^p \not\equiv a \pmod{p}$. Then

$$(\exists n \in \mathbf{N})(2 \leq n \leq p - 1 \ \& \ n \mid p).$$

This theorem is usually proved by proving the contrapositive: if p is prime, then for all integers a , it is true that $a^p \equiv a \pmod{p}$. I suspect the intuitionists would accept this proof, because statement and proof can be phrased in such a way that they refer only to the finite set $\{1, 2, \dots, p\}$.

Example 3. Pick any programming language, and let F be the set of functions $f: \mathbf{N} \rightarrow \mathbf{N}$ for which there is a program in this programming language. Then F is denumerable (because the set of all programs is denumerable), so classically, there exists a bijection $\mathbf{N} \leftrightarrow F$, because the assertion that there is no such bijection leads to a contradiction and is therefore false. However, it turns out to be impossible actually to exhibit one! I suspect that the intuitionists, if they lapsed so far from orthodoxy as to permit themselves to discuss denumerable sets, would find that this fact makes F is *provably nondenumerable*.

I need to preface the next example with some definitions. A *total order* on a set S , roughly speaking,¹ is a choice, for each pair of elements, which is larger. (Examples are the ordinary orders on \mathbf{N} , \mathbf{Z} , \mathbf{Q} , and \mathbf{R} .) A total order is a *well order* if it has the additional property that every nonempty subset of S contains a smallest element. (Thus, of the usual total orders on \mathbf{N} , \mathbf{Z} , \mathbf{Q} and \mathbf{R} , the only one that is a well order is the one on \mathbf{N} .)

Example 4. In naïve set theory, one can prove (by contradiction) that there exists a well order for every nonempty set.

Since the proof of this assertion is a proof by contradiction, and the intuitionists certainly do not accept it. Their case here is strengthened by the interesting fact that *no* classical mathematician has ever succeeded in exhibiting *even one* well order on any nondenumerably infinite set.

Example 5. Let Q be the statement: "There exist irrational numbers α and β for which α^β is rational." This is easily proven by classical mathematics. Let

$$x := \sqrt{2}^{\sqrt{2}}; \tag{1}$$

either x is rational or irrational. If x is rational, then one can take $\alpha = \beta = \sqrt{2}$; on the other hand, if x is irrational, we have

$$x^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2, \tag{2}$$

so that one can take $\alpha = x$ and $\beta = \sqrt{2}$. Thus (to the classical mathematician) either (1) or (2) provides the dispositive example. For the intuitionist, however, this demonstrates nothing of the sort, since neither (1) nor (2) has been proved to be an example. (S)he would insist on having a proof of the rationality/irrationality of x —an unsolved problem—before allowing that an example had been found.

¹ Precisely: it is a binary relation R that is transitive and that has the property: for each $s, t \in S$, exactly one of $\left\{ \begin{array}{l} sRt \\ s = t \\ tRs \end{array} \right\}$ holds.