Every Integer Is Either Even Or Odd

Lucilla

Abstract

While the statement in this paper's title is hardly astonishing, what *is* astonishing is how difficult it is to prove without making use of mathematical induction. Either that or Lucilla is bad at math.

0 Introduction

Let $n \in \mathbb{Z}$. We define

$$\begin{cases} n \text{ is even} & \Leftrightarrow \quad \exists k \in \mathbb{Z} : \; n = 2k \\ n \text{ is odd} & \Leftrightarrow \quad \exists k \in \mathbb{Z} : \; n = 2k+1 \end{cases}$$

The goal of this paper is to prove the statement

$$\forall n \in \mathbb{Z} : \; n \text{ is even} \;\otimes\; n \text{ is odd}$$

(where $\otimes$ denotes XOR, i.e. every integer is either even or odd; never both, never neither). We will accomplish this in two steps, by proving two separate statements:

$$\begin{cases} \forall n \in \mathbb{Z} : & \neg(n \text{ is even} \;\wedge\; n \text{ is odd}) \\ \forall n \in \mathbb{Z} : & n \text{ is even} \;\vee\; n \text{ is odd} \end{cases}$$

thus firstly that no integer can be both even and odd at the same time, and secondly that no integer can be neither even nor odd at the same time.

It turns out that, while the truth of the first statement (henceforth affectionately named **NAND**) can be easily shown, the second (henceforth called **OR**) requires considerably more effort if you avoid using mathematical induction for it. This paper aims to present just such a proof, of which the reader is implored to find one of their own if they feel up to it before continuing.

1 NAND

The proof (of both substatements) makes heavy use of a lemma about integers, which, in the tradition of giving them funny names, will be referred to as the *fence post lemma*:

Lemma fence-post-lemma

Any two distinct integers differ by at least 1.

The truth of this is so clear as to not even deserve being mentioned. Should, however, a reader find it not obvious, they shall find a proof at the end of this paper.

With no more than that, we are already able to prove **NAND**:

Theorem NAND

No integer is both even and odd at the same time.

Proof. We proceed by contradiction. Suppose that there does exist an integer n which is both even and odd. Then there exist integers k and l such that

$$n = 2k \ \wedge \ n = 2l + 1.$$

Equating the right-hand sides, we find that $2k = 2l + 1$; dividing both sides by 2, we obtain that $k = l + 1/2$. Thus k and l are two integers that differ by $1/2$. k and l are obviously not equal, otherwise $2k = 2l + 1$ would imply $0 = 1$. Thus they must be distinct, and since they differ by less than 1, this is a contradiction to the fence post lemma. □

That was fast, but let us not rest on our laurels, for the real difficult part is yet to come. We just did the easy bit.

2 OR

We begin with a few definitions from elementary real analysis.

Definition inf, sup

The *infimum* of a non-empty set S of real numbers, denoted $\inf S$, is a real number a satisfying the conditions

- $\forall x \in S: \ a \leq x;$
- $\forall b \in \mathbb{R}: \ (\forall x \in S: \ b \leq x) \Rightarrow b \leq a,$

if a number satisfying the first condition exists. In other words, the infimum is the largest lower bound of the set S, if one exists.

The *supremum*, denoted $\sup S$, is similarly defined by replacing $\leq$ with $\geq$ in the definition above, and is the smallest upper bound of S, if one exists.

If a is the infimum of S and additionally $a \in S$, then a is called the *minimum* of S. Similarly, the supremum of S, if an element of S, is called the *maximum* of S.

It's not difficult to see that infima (and suprema) are unique: let a and b both be numbers that satisfy both conditions for an infimum, then it follows from the second condition that $a \leq b$ and $b \leq a$, thus $a = b$.

Also, if an infimum (supremum) is a minimum (maximum), then it suffices to check for the first condition, since the second automatically follows: let $a \leq x$ for all $x \in S$ and further let $a \in S$. Then for every b such that $b \leq x$ for all $x \in S$, in particular $a \in S$, so $b \leq a$.

For some particularly well-behaved sets, it can be easily shown that an infimum is necessarily a minimum (and likewise that a supremum is necessarily a maximum). For instance, the infimum of a *finite* set is always a minimum: one can show this by running the minimum-finding algorithm on the set, which will terminate after finitely many steps, and return a number less than or equal to every element of the set and itself in the set. We will instead show this property for sets of *integers*:

Lemma integer-inf-is-min

Let S be a set of integers. Then $\inf S$, if it exists, is a minimum of S.

Proof. Suppose the infimum of S is a. We will show that, firstly, $\lceil a \rceil$ (a rounded up to the nearest integer) also satisfies $\lceil a \rceil \leq x$ for all $x \in S$ (and that therefore $a = \lceil a \rceil$), and secondly, that $\lceil a \rceil \in S$.

Suppose a is a lower bound of S, but $\lceil a \rceil$ isn't. It follows there exists an integer n in S with $a \leq n$ and $\lceil a \rceil > n$. Since the difference between x and $\lceil x \rceil$ is less than 1, it follows that n and $\lceil a \rceil$, both integers, must differ by less than 1, which contradicts the fence post lemma.

Thus $\lceil a \rceil$ is also a lower bound of S. Because a is an infimum of S, it follows that $\lceil a \rceil \leq a$. But $\lceil a \rceil \geq a$ obviously because of the rounding-up function. Thus $\lceil a \rceil = a$.

We now show $\lceil a \rceil \in S$. Suppose $\lceil a \rceil \notin S$. Then $\lceil a \rceil < x$ for all $x \in S$ ("$<$" means "$\leq$, but not $=$"), but since $\lceil a \rceil$ and all $x \in S$ are integers, by the fence post lemma, they must differ by at least 1, which means $\lceil a \rceil \leq x - 1$ for all $x \in S$. But then $\lceil a \rceil + 1$ is a bigger lower bound of S, a contradiction. □

With this lemma (whose truth for suprema and maxima is proved analogously), we can finally tackle the monster that is **OR**:

Theorem OR

Every integer is even or odd.

Proof. Suppose there exists an integer n which is neither even nor odd, thus for all integers m it holds that $2m \neq n$ and $2m + 1 \neq n$.

Consider $E = \{m \in \mathbb{Z} : \; 2m \leq n\}$ and $k = \sup E$. Because k is the supremum of a set of integers, k is a maximum and thus itself an integer. Since $k \in E$, it follows that $2k \leq n$. Because n is not even, $2k \neq n$, thus $2k < n$. Since k is the maximum of E, $k+1$ is not in E, thus $2(k+1) = 2k+2 > n$. Overall we have $n \in]2k, 2k+2[$.

Moreover, $n \neq 2k+1$, since n is not odd, so we have two cases: either $n \in]2k, 2k+1[$ or $n \in]2k+1, 2k+2[$. Both are open intervals of length 1, which means n must be distinct from both of its limiting values, and must have distance less than 1 to both of them. But they are both integers, and so is n. This is a contradiction to the fence post lemma. □

Phew!

3 Addendum

As promised, a proof of the fence post lemma, for those curious to know:

Lemma fence-post-lemma

Any two distinct integers differ by at least 1.

Proof. Let k and l be two integers and $k \neq l$. Thus $k - l \neq 0$. Because the absolute value is a norm on $\mathbb{R}$, it follows $|k - l| > 0$. But the difference of two integers is an integer, and since the absolute value can at most negate the sign of its argument, which still produces an integer, it follows $|k - l|$ is a (positive) integer. The smallest positive integer is 1. □

And finally, a baby-easy proof of **OR** using mathematical induction. The reader is implored to imagine it being read in a schoolchild's monotonous voice.

Theorem OR-inductive

Every integer is even or odd.

Proof. We first show the statement for all $n \in \mathbb{N}$.

The base case is $n = 0$. 0 is even, as there exists an integer k (namely 0) with $0 = 2k$.

For the induction step, let n be even or odd. Suppose n is even, with $n = 2k$; then $n + 1 = 2k + 1$ is odd. Suppose instead that n is odd, with $n = 2k + 1$; then $n + 1 = 2k + 2 = 2(k + 1)$ is even. Thus n being even or odd implies $n + 1$ being even or odd.

Finally we show the statement for all $n \in \mathbb{Z}$ by proving that if n is even or odd, then $-n$ is.

Suppose n is even, with $n = 2k$; then $-n = -2k = 2(-k)$ is even. Suppose instead that n is odd, with $n = 2k + 1$; then $-n = -(2k + 1) = -2k - 1 = 2(-k - 1) + 1$ is odd. Thus n being even or odd implies $-n$ being even or odd.

Since $\mathbb{Z} = \mathbb{N} \cup \{-n : n \in \mathbb{N}\}$, the result follows. □