"Don't just read it; fight it! Ask your own questions, look for your own examples, discover your own proofs..."

Paul Halmos

# All Natural Numbers are either Even or Odd

James Smith
james.smith@openmathematics.org

February 17, 2020

# Meaning versus representation (I)

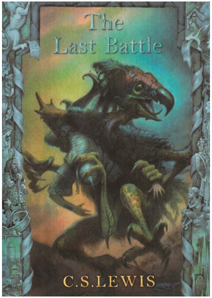
"...suppose there in fact existed a wonderful correspondence between our concepts and the world...whereby it was in fact metaphysically impossible for certain claims constitutive of those concepts not to be true. This is, of course, not implausible in the case of logic and arithmetic..."

Stanford Encyclopedia of Philosophy

# Meaning versus representation (II)

What is a concept?

If I asked you if you have read The Last Battle by C.S.Lewis...




...clearly I am not referring to my own hard copy (brandishes book).

# Meaning versus representation (III)

The Last Battle by C.S.Lewis is a concept.

Concepts are ubiquitous. How many are there in just these first few slides? The concept of a book, the concepts of reading and writing, the concept of time, the concept of a concept itself.

The concepts that we communicate amongst ourselves and can largely agree upon I call *general* concepts.

# Meaning versus representation (IV)

How do we frame and communicate general concepts?

In natural languages we employ words and punctuation composed into terms, phrases or expressions. So there is a dichotomy:

$$\begin{tikzcd} \text{General concept} \arrow[r, bend left, "\text{gives meaning to}"] & \begin{array}{l}\text{Corresponding term,}\\ \text{phrase or expression}\end{array} \arrow[l, bend left, "\text{is representative of}"] \end{tikzcd}$$

# Meaning versus representation (V)

In the field of symbolic reasoning, which encompasses logic and mathematics, we mostly use symbols in preference to words.

$$\begin{tikzcd} \text{General concept of pi} \arrow[r, bend left, "\text{gives meaning to}"] & \pi \arrow[l, bend left, "\text{is representative of}"] \end{tikzcd}$$

Notice that the general concept of pi is not on the left at all! It is just one of the natural language phrases we use to represent it.

# Meaning versus representation (VI)

So good is natural language at communicating general concepts that we scarcely notice the difference between them and their representations at all.

What if I switched languages to French, however, or used an emoji than the corresponding natural language phrase? Only then does the difference become apparent.

So is this our wonderful correspondence? Unfortunately not.

The correspondence that Stanford speaks of is not between general concepts on the one hand and their representations on the other.

It is between general concepts and reality (whatever that is).

# Meaning versus representation (VII)

Can we get a handle on reality? This is debatable, which is why the quote from Stanford is couched as a supposition.

The point is that certain things might be considered to be universal in the sense that they exist regardless of our conception of them. And in mathematics and logic, this is considered more likely.

The concept of pi might be considered universal, for example, or the concept of a natural number.

But, as I have said, this is debatable.

# Meaning versus representation (VIII)

Thus in symbolic reasoning we should attempt a less lofty goal.

We should invent symbols, or occasionally resort to words, to represent only our general concepts, and not claim that these symbols or words are representative of universal concepts.

We should leave attempts at universal reasoning to philosophers!

Which is not to belittle their efforts, by the way. To arrive at this conclusion was surely a philosophical exercise.

# Meaning versus representation (IX)

Maybe you think all of this philosophising is pretty aimless...

The lack of an understanding of the dichotomy between meaning and representation led to problems that continue to this day, however, not least in mathematics and logic.

Mathematicians routinely introduce symbols to represent general concepts without realising that they are doing so.

They tend not to be satisfied with these general concepts, however, and habitually equate them with other general concepts in a dubious attempt to legitimise them.

The classic example is the identification of the natural number zero with the empty set.

# Meaning versus representation (X)

Perhaps if mathematicians could be persuaded to explicitly declare the symbols that they subsequently employed, they might realise that there is no need to do anything more.

Pi is just pi. There is no justification in equating it an equivalence class of Cauchy sequences of rational numbers, that itself boils down to nothing but a hugely complex set.

"Everything is a set...even though it would take a considerable amount of work to write a complete formula...in set theory that expresses the notion $x$ is a scheme, it is possible to do so. The same thing should be true for any mathematical object."

The Stacks Project

I will come back to the "Everything is a Set" view later on.

# Peano's axioms (I)

What are Peano's axioms? We deliberately use non-mathematical language to begin with. We will need the following concepts...

- the concept of a objects,
- the concept of a successor,
- the concept of equality.

The second through to the fifth axioms just define equality in the standard way and are of no further interest.

# Peano's axioms (II)

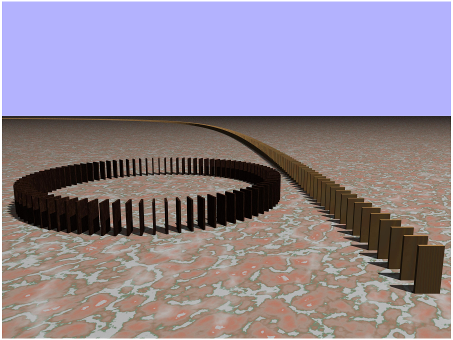
Here is the essence of the remaining axioms:

- 6. Every natural number has a successor.
- 7. Any two natural numbers that have the same successor must in fact be the same, and vice versa.
- 1+8 There is a unique natural number which is not the successor of any other natural number.

The ninth axiom is something special and is the main subject of these slides. It is left off for now but we will come to it shortly.

# Peano's axioms (III)

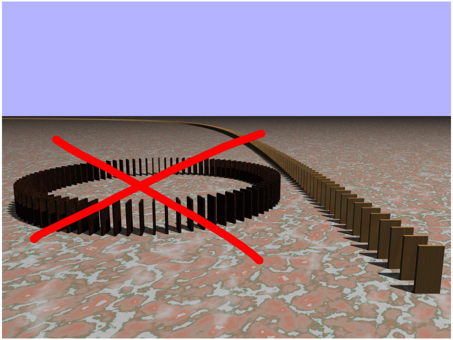
Below is a representation of the natural numbers. One domino is considered to be the successor of another if it stands directly behind it.



These dominoes obey the first eight of Peano's axioms. It is a worthwhile exercise to verify this. Just check axioms 6, 7 and 1+8.

# Peano's axioms (IV)

Notice that we have this henge of dominoes. Unfortunately their inclusion does not break the first eight of Peano's axioms. You could double check this. Bah!



This is where the ninth axiom comes in. It effectively rules out the henge of dominoes...

# The Principle of Induction (I)

Before introducing the ninth axiom, we introduce two more concepts in order to make the language a little more intuitive:

- The concept of counting. To count is to go from one object to its successor and so on.
- Recall that we have a unique object which is not the successor of any other. We call this the first object.

Now for the ninth axiom, the Principle of Induction:

| |
|---|
| All of the natural numbers can be reached by starting at the first natural number and counting. |

# The Principle of Induction (II)

It should be easy to see now that why Principle of Induction rules out the henge of dominoes...

- Because the first domino is not in the henge;
- and because no domino in the henge is the successor of any domino outside of it;
- we can never reach any domino in the henge by starting at the first domino and counting.

So if our dominoes are to obey the Principle of Induction, and therefore be considered a representation of the natural numbers, they cannot include a henge of dominoes.

# The Principle of Induction (III)

Sceptical? Perhaps you are used to seeing the Principle of Induction written in this form:

$$\left.\begin{array}{r} P(0) \\ \forall k\,(P(k) \Rightarrow P(k+1)) \end{array}\right\} \Rightarrow \forall n P(n)$$

We use the notation $k+1$ for the successor of $k$ here. We also note the presence of universal quantification, but pay no more attention to it for the time being.

We really can translate this back into the language dominoes and henges...

# The Principle of Induction (IV)

In order to see this, we visualise a statement $P(n)$ holding by way of the corresponding domino being lightly coloured. So regardless of what $P(n)$ actually is, we imagine it corresponds to the statement:

"the $n$'th domino is lightly coloured"

Now the Principle of Induction reads:

> If the first domino is lightly coloured; and if any domino being lightly coloured implies that its successor is lightly coloured; then these two statements taken together imply that all dominoes are lightly coloured.

# The Principle of Induction (V)

Again we can prove that the Principle of Induction rules out the henge of dominoes...

- It is certainly true that the first domino is lightly coloured;
- and it is also true that any domino being lightly coloured implies that its successor is lightly coloured;
- but we cannot claim that these two statements taken together imply that all dominoes are lightly coloured unless we rule out the henge of darker dominoes.

I cannot stress enough that the essence of the Principle of Induction lies in dominoes and henges! It is simply there to rule out the henges!

# The set-theoretic representation of the natural numbers (I)

Are there representations of the natural numbers that are a bit more mathematical? The commonly accepted set-theoretic representation can be defined somewhat informally:

- $0 = \emptyset$
- $1 = 0 \cup \{0\} = \{0\}$
- $2 = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$ ...

Here $n + 1$ is defined as $n \cup \{n\}$. Note that we also have...

$$n + 1 = \{0, 1..., n\}$$

It is possible to check that this representation obeys the first eight of Peano's axioms. Again just check axioms 6, 7 and 1+8.

# The set-theoretic representation of the natural numbers (II)

What about the Principle of Induction? In set-theoretic form it is:

$$\left.\begin{array}{r} P(0) \\ \forall k\in\mathbb{N}\ (P(k) \Rightarrow P(k+1)) \end{array}\right\} \Rightarrow \forall n\in\mathbb{N}\ P(n)$$

Russell's paradox teaches us that we cannot quantify universally without selecting from an existing set, hence the need for this set called $\mathbb{N}$. But how do we define it?

Suppose we have a set $I$ which contains all the sets that represent natural numbers. It may contain other sets, too, but we pretend that doesn't matter. And suppose we could define a property $N(n)$ that identifies just the sets that represent natural numbers. Then the following definition would suffice:

$$\mathbb{N} = \{n \in I \mid N(n)\}$$

# The set-theoretic representation of the natural numbers (III)

What is this mystery set $I$ from which we can select all those sets that represent the natural numbers? It is called an inductive set and it has the following properties:

- $\emptyset \in I$
- If $n \in I$ then $n + 1 \in I$

It turns out that there is no way to form an inductive set without the axiom of infinity, which simply asserts that one exists.

Moreover, in practice a formal definition of $N(n)$ is overlooked and the following is preferred:

$$\mathbb{N} = \{n \in I \mid n \in I' \text{ for every inductive set } I'\}$$

From this we can prove that $\mathbb{N}$ is the smallest inductive set.

# The set-theoretic representation of the natural numbers (IV)

Here is the Principle of Induction again. This time we prove it, relying on the fact that $\mathbb{N}$ is the smallest inductive set...

$$\left.\begin{array}{r} P(0) \\ \forall k \in \mathbb{N}\, (P(k) \Rightarrow P(k+1)) \end{array}\right\} \Rightarrow \forall n \in \mathbb{N}\; P(n)$$

We define the set $A$ to be $\{n \in \mathbb{N} \mid P(n)\}$. Clearly we have $A \subseteq \mathbb{N}$. But $A$ is also inductive by definition and since $\mathbb{N}$ is the smallest inductive set we have $\mathbb{N} \subseteq A$. So $A = \mathbb{N}$ and we're done.

Now we have a set $\mathbb{N}$ of sets that obey all of Peano's axioms and we really can say, therefore, that they are a representation of the natural numbers.

# The set-theoretic representation of the natural numbers (V)

Aside from the fact that the "smallest inductive set" approach seems suspect, there are other issues with the set-theoretic representation of the natural numbers...

One is that we get additional behaviour that we don't want. For example, the intersection $1 \cap 2$ makes sense, but should it?

The other is that these sets are often identified with the natural numbers rather than being considered just a representation of them. Recall the following identity given earlier:

$$0 = \emptyset$$

Many, including me, would argue that it simply does not make sense to equate these two concepts.

# A modern approach

It is easy to criticise the identification of the natural numbers as sets, and, by extension, the "everything is a set" view. But it would be churlish not to acknowledge that it was an enormous advance at the time. I am told it brought about the unification of mathematics, which up until that time had been a bit of a disparate mess.

A better and more conciliatory approach is to try to figure out what concepts the proponents of this view missed at the time and then to ask, if they had these to hand, what might they have come up with instead? These concepts spring to mind:

- Types
- Terms and constructors
- Variables and quantification
- Intuitionistic proofs and contexts

# Types

We return to the aforementioned equation identifying the natural number zero and the empty set:

$$0 = \emptyset$$

Why exactly does it not make sense? The reason is that zero is a natural number and the empty set is, well, a set. And you cannot equate two concepts that are fundamentally different.

So we come to the concept of a type. All natural numbers have the same type, which is different to the type of all sets. And from the concept of a type comes the principle that we cannot equate two objects if they have different types. Therefore the above equation is disallowed, we say that it is not well typed.

As Larry Paulson once wrote, types stop us writing nonsense.

# Terms and constructors (I)

Like their allies, variables, terms are so ubiquitous that it is far from immediately obvious that they are constitute a concept in their own right. Let us go over the philosophical ground again...

Consider zero. Peano showed that it can be defined in a general but nonetheless precise way, however we have struggled to find a convincing way of representing it.

But why not just take the word 'zero'? It is totally unambiguous, nor is it a domino or a set. This is what we call a term.

If we represent a general concept by a term, we say that its meaning is the general concept.

# Terms and constructors (II)

Terms are defined using constructors and always have a type:

```
Type NaturalNumber

Constructor zero:NaturalNumber
```

Here we have defined a type followed by a nullary constructor of that type. Nullary constructors take no arguments, so when you define a nullary constructor, you are effectively defining a term.

Now we have a term for zero with the right type:

```
zero \\ 0

zero:NaturalNumber \\ holds
```

# Terms and constructors (III)

Constructors also allow us to form composite terms. The unary constructor below takes one argument, namely any other term of type `NaturalNumber`, and results in another term of that type:

```
Constructor successor(NaturalNumber):NaturalNumber
```

Now we can construct the terms representing the next few natural numbers:

```
successor(zero) // 1
successor(successor(zero)) // 2
successor(successor(successor(zero))) // 3
...
```

Bear in mind that constructors are not functions, they are a purely syntactic device.

# Variables and quantification (I)

Variables are another concept that mathematicians use all the time but rarely define explicitly. Consider the following:

```
Type RealNumber
Variable x:RealNumber
Constructor f(RealNumber):RealNumber
```

These definitions mean that the term `f(x)` make sense, we say that it is well formed. In fact variables are considered to be terms in their own right, which is why we can pass them as arguments to constructors in order to form other terms.

Again bear in mind that the term `f(x)` has nothing to do with any function. The example here was chosen to make you think. If we wanted it to represent the value obtained from the application of some function `f` to the variable `x`, we would have to define this meaning explicitly.

# Variables and quantification (II)

To continue, unless we assign a value to a variable, it is considered to be undefined. If a statement containing a variable holds when that variable is undefined, it seems reasonable to say that it holds for all values of that variable. So the following two statements...

```
x is undefined
x=x
```

...are equivalent to:

```
∀x x=x
```

The concept of variables being undefined, therefore, is effectively synonymous with universal quantification. Indeed, as long as doing so does not lead to ambiguity, it is often permissible to leave out universal quantification altogether.

# Intuitionistic proofs and contexts (I)

You may have noticed that there has never been any mention of a statement being true or false, only of a statement holding. In fact the concepts of truth and falsity have not been used at all. This is quite deliberate.

From an Aristotelian point of view, statements can be evaluated or interpreted as being true or false. From an intuitionistic point of view, however, a statement holds either if it has been stated by way of an axiom, or it has been proven. We can say in either case that it is true for the sake of emphasis, but this is only a turn of phrase.

You could say that any theorem is a syntactic consequence of certain axioms or theorems, in order to emphasise that there is no underlying model or interpretation at work.

# Intuitionistic proofs and contexts (II)

Suppose we have a theorem called `TwoIsEven`. This relies on other axioms and theorems, which we make use of by inserting their statements together with references to their labels:

```
Theorem (TwoIsEven)
  2:Even
  Proof
    1:Odd from OneIsOdd
    s(1):Even from SuccessorsOfOddsAreEven
  Conclusion
    2:Even from TheSuccessorOfOneIsTwo
```

The details of the proof of the `SuccessorsOfOddsAreEven` theorem are irrelevant here. We simply employ the statement and justify it by referencing the theorem's label with the `from` keyword.

# Intuitionistic proofs and contexts (III)

It is helpful, although strictly speaking not quite right, to think of a context as a mapping from labels to statements:

```
OneIsOdd :: 1:Odd,
TheSuccessorOfOneIsTwo :: s(1)=2,
SuccessorsOfOddsAreEven :: ...
```

Since this context permits us prove that two is indeed an even number, we write:

OneIsOdd :: 1:Odd, TheSuccessor... $\vdash$ TwoIsEven :: 2:Even

In general, if $\pi$ is some context which permits us to prove some statement $P$ and we label the theorem $p$, then we write:

$$\pi \vdash p :: P$$

Perhaps using the symbol $\pi$ was a bad choice...

# A type theoretic representation of the natural numbers

With types, terms and so on to hand, we can now formulate what we call a construction of the natural numbers. However, unlike the set-theoretic representation, there is nothing contrived about it:

```
Type NaturalNumber
Constructor zero:NaturalNumber
Constructor successor(NaturalNumber):NaturalNumber
```

It should be straightforward to check that this construction obeys Peano's axioms. Just check axioms 6,7 and 1+8 as usual.

# The Principle of Induction in type-theoretic form (I)

What about the Principle of Induction? The first thing to do is to state it in the language of types, terms, contexts and so on.

$$\frac{\rho \vdash R :: P(z) \quad \sigma(k) \vdash S(k) :: P(k) \Rightarrow P(s(k))}{\tau(n) \vdash T(n) :: P(n)}$$

Hopefully it does not look too daunting!

We can actually *derive* this from the construction of the natural numbers just given. In order to do so, we need to find out what $\tau(n)$ and $T(n)$ are. How can we achieve this?

# The Principle of Induction in type-theoretic form (II)

Returning to the representation using dominoes, the first thing to realise is that we have constructed only the lighter coloured ones. To make this clear, we explicitly construct the darker ones, too:

```
Type N
Constructors z:N, s(N):N, w:N
Axiom s(s(s(s(s(s(s(s(s(s(w))))))))))=w
```

Here the darker dominoes start with `w` and the axiom equating the tenth successor with `w` gives us a henge with ten dominoes. The original henge was bigger but you get the idea.

The point is, however, that have have not created this additional henge of darker dominoes in our original construction! We have only constructed the lighter coloured ones!

# All natural numbers are either even or odd (I)

In order to demonstrate how to derive the Principle of Induction, we utilise a concrete example, namely proving that all natural numbers are either even or odd.

We begin with some definitions:

```
Type EvenOrOdd
Types Even,Odd:EvenOrOdd

Axiom (EvensAreDivisibleByTwo)
  n:Even iff 2|n

Axiom (SuccessorsOfOddsAreEven)
  n:Odd iff s(n):Even

Axiom (EvenOrOddsAreEitherEvensOrOdds)
  n:EvenOrOdd iff n:Even ∨ n:Odd
```

# All natural numbers are either even or odd (II)

Next, a simple theorem for the base case:

```
Theorem (ZeroIsEvenOrOdd)
  z:EvenOrOdd
  Proof
    2|z
    z:Even from EvensAreDivisibleByTwo
    z:Even ∨ z:Odd by RightDisjunctionIntroduction
  Conclusion
    z:EvenOrOdd from EvenOrOddsAreEitherEvenOrOdd
```

Note that we have referenced two of the previous axioms, as expected. We have also referenced the inference rule for right disjunction introduction here by way of the `by` keyword.

# All natural numbers are either even or odd (III)

Now the theorem for the induction step, somewhat incomplete:

```
Theorem (SuccessorsOfEvenOrOddsAreEvenOrOdd(k))
  k:EvenOrOdd => s(k):EvenOrOdd
  Proof
    Suppose
      k:EvenOrOdd
    Then
      k:Even ∨ k:Odd from EvenOrOddsAreEitherEvenOrOdd
      Suppose
        k:Even
      Hence
        s(k):Odd from SuccessorsOfEvensAreOdd
      k:Even => s(k):Odd by ConditionalProof
      ...
    Hence
      s(k):EvenOrOdd by ProofByCases
  Conclusion
    k:EvenOrOdd => s(k):EvenOrOdd
```

# All natural numbers are either even or odd (IV)

To summarise so far, we have the base case and the induction step:

$$\rho \vdash R :: P(z)$$

$$\sigma(k) \vdash S(k) :: P(k) \Rightarrow P(s(k))$$

Recall that we need to find out what $\tau(n)$ and $T(n)$ are. We start with a template theorem and an empty proof for $\tau(z)$ and $T(z)$:

```
Theorem (NaturalNumbersAreEvenOrOdd(z))
  z:EvenOrOdd
  Proof
    ...
  Conclusion
    z:EvenOrOdd
```

So what is the context, and what is the proof?

# All natural numbers are either even or odd (V)

We obviously need to make use of the base case. We know that the theorem `ZeroIsEvenOrOdd` proves the statement `z:EvenOrOdd`, so the context must be:

```
ZeroIsEvenOrOdd :: z:EvenOrOdd
```

So there is effectively no need for a proof:

```
Theorem (NaturalNumbersAreEvenOrOdd(z))
  z:EvenOrOdd
  Conclusion
    z:EvenOrOdd from ZeroIsEvenOrOdd
```

Neat!

In the general case, setting $\tau(z) = R :: P(z)$ gives us:

$$\tau(z) \vdash T(z) :: P(z)$$

# All natural numbers are either even or odd (VI)

What is the context $\tau(s(k))$ and theorem $T(s(k))$? We again start with a template theorem with an empty proof:

```
Theorem (NaturalNumbersAreEvenOrOdd(s(k)))
  s(k):EvenOrOdd
  Proof
    ...
  Conclusion
    s(k):EvenOrOdd
```

Recall that we have the induction step to hand, which implies that if `k` is an even or odd number then `s(k)` is an even or odd number:

```
Successors...(k) :: k:EvenOrOdd=>s(k):EvenOrOdd
```

# All natural numbers are either even or odd (VII)

The first devious bit...

If we are to make use of the induction step in order to assert the consequent, namely the statement `s(k):EvenOrOdd`, we must assert the antecedent, namely the statement `k:EvenOrOdd`.

The second devious bit...

By what right are we able to assert `k:EvenOrOdd`? Well, the proof of this can only be `NaturalNumbersAreEvenOrOdd(k)`. So our context has to be recursive:

```
NaturalNumbersAreEvenOrOdd(k) :: k:EvenOrOdd,
Successors...(k) :: k:EvenOrOdd => s(k):EvenOrOdd
```

If this seems a bit strange, remember that we haven't worked out the proof of `NaturalNumbersAreEvenOrOdd(k)` yet!

# All natural numbers are either even or odd (VIII)

If you think about it, the theorem has to take this form:

```
Theorem (NaturalNumbersAreEvenOrOdd(s(k))
  s(k):EvenOrOdd
  Proof
    k:EvenOrOdd from NaturalNumbersAreEvenOrOdd(k)
    k:EvenOrOdd => s(k):EvenOrOdd from Successors...(k)
  Conclusion
    s(k):EvenOrOdd by ModusPonens
```

Again, pretty neat.

So, in a similar vein to before, in the general case we set:

$$\tau(s(k)) = T(k) :: P(k), S(k) :: P(k) => P(s(k))$$

This gives us:

$$\tau(s(k)) \vdash T(s(k)) :: P(s(k))$$

# Parameterising contexts and labels (I)

Before moving on, we should note a new concept that has been utilised along the way, namely the use of parameters in contexts and labels.

You might ask why it is necessary to parameterise the context and the label of the induction step. The following surely should suffice:

$$\sigma \vdash S :: P(k) \Rightarrow P(s(k))$$

The answer is that we probably could get away without parameters here. After all, normally when proving things by induction we just refer to "the induction step", which is really just an informal label and obviously doesn't have a $k$ in it.

# Parameterising contexts and labels (II)

In other situations, however, parameters are unavoidable. Recall that we have proved the following:

$$\tau(z) \vdash T(z) :: P(z) \quad \tau(s(k)) \vdash T(s(k)) :: P(s(k))$$

Here the contexts $\tau(z)$ and $\tau(s(k))$ are markedly different, as are the theorems $T(z)$ and $T(s(k))$. But in the end we will need to use the metavariables $\tau$ and $T$ with generality. Hence the need to parameterise them.

Note that the value of the parameter in the first case, the one that corresponds to the base case, is just the term $z$. And for the other case, the one that corresponds to the induction step, it has been deliberately chosen to be the term $s(k)$ and not, as you might first expect, just $k$. This keeps the two cases separate.

# Metatheorems (I)

The other concept that has not been utilised yet, but has been implicit in the argument so far, is the concept of a metatheorem.

Recall that we have concrete examples for all of the requisite contexts and theorems. The concrete example for $T(z)$ is, again:

```
Theorem (NaturalNumbersAreEvenOrOdd(z))
  z:EvenOrOdd
  Conclusion
    z:EvenOrOdd from ZeroIsEvenOrOdd
```

Now let's generalise it, replacing the label with $T(z)$, etc:

```
Metatheorem (T(z))
  P(z)
  Conclusion
    P(z) from R
```

# Metatheorems (II)

And for the other theorem, replacing the label $T(s(k))$, etc.

```
Metatheorem (T(s(k)))
  P(s(k))
  Proof
    P(k) from T(k)
    P(k) => P(s(k)) from S(k)
  Therefore
    P(s(k)) by ModusPonens
```

Now the structure of both proofs, and their use of contexts, really stands out. Especially this second one.

Think about it. In order to prove that 3 is even or odd, say, you suppose that 2 is even or odd and then use the induction step. This is exactly what is going on above.

# All natural numbers are either even or odd (IX)

Here we take the premises and define the contexts as expected. Recall that we have the two metatheorems to hand, so the lines after the context definitions can be verified:

```
Rule (Induction)
  Premises
    ρ ⊢ R::P(z)
    σ(k) ⊢ S(k)::P(k) => P(s(k))
  Proof
    let τ(z) = R::P(z)
    let τ(s(k)) = S(k)::P(k) => P(s(k)), T(k)::P(k)
    ...
  Therefore
    τ(n) ⊢ T(n)::P(n) by ProofByCases
```

Note that we are proving an inference rule and not a theorem, since we want to be able to state "by induction".

# All natural numbers are either even or odd (X)

Lastly we fill in the remainder of the proof:

```
n=z ∨ n=s(k)
Suppose
  n=z
Then
  τ(z) ⊢ T(z)::P(z)
Hence
  τ(n) ⊢ T(n)::P(n)
n=z => T(n) ⊢ T(n)::P(n)
Suppose
  n=s(k)
Then
  τ(s(k)) ⊢ T(s(k))::P(s(k))
Hence
  τ(n) ⊢ T(n)::P(n)
n=s(k) => T(n) ⊢ T(n)::P(n)
```

# Conclusion

Let's make use of our new inference rule:

```
Theorem (NaturalNumbersAreEvenOrOdd(n))
  Premises
    ZeroIsEvenOrOdd :: z:EvenOrOdd
    Successors...(k) :: k:EvenOrOdd => s(k):EvenOrOdd
  Conclusion
    n:EvenOrOdd by Induction
```

One bonus is that we don't have to give the contexts for the base case and induction step explicitly. If needed, the verifier would be able infer them easily enough but in fact they are not needed.

So the form of the theorem is ideal, exactly what you write down with pen and paper, albeit formally.

"Of course, what we think of as knowledge is always based on our best efforts in the past to establish what is more likely than not to be true, but it is inevitably combined with a legacy of accumulated error sanctified by repetition, and we have learned that our constant asymptotic progress toward Veritas requires that reason be used to subject the authority of knowledge to continuous challenge."

Al Gore