Dear Paolo! Diez, Sept. 19, 2007

Considering our pleasant meeting half a year ago in München and the privatissimum you gave me there, and after re-reading the relevant sections in (Bussotti, 2006), I am still not absolutely sure on what you exactly mean with *indefinite descent* and *reduction-descent*. The weakness of (Bussotti, 2006) in this point of differentiation is the following. You give only an extensional account of the two notions, but this account differs from page to page. Moreover, you state that you have a clear intuition of the difference in intensional terms, but you do not define the two notions intensionally. I cannot work with such notions. So I will try to find an intensional definition here.

To make sure that we mean exactly the same with the two notions, I will describe my view on induction here in very detail. I see no other way to become certain that the two names denote the same notions for both of us.

I hope that you agree with the following or even consider it all to be trivial. Then we could go on with our joint paper.

# 1 Logic

For me there is only one single general form of mathematical induction. I recognize its applications at any times in the known history of mathematics, from Hippasus over Euclid to Fermat.

Behind several lingual forms of presentation, there is a single logical basis to this, which is the Theorem of Nötherian Induction ($\mathsf{N}$), based on the notion of well-foundedness $\mathsf{Wellf}(<)$. A relation $<$ is *well-founded* if any non-empty set has a minimal element, i.e. an element $m$ for which there is no other element $w$ with $w<m$. Note that a total (i.e., linear) irreflexive ordering $<$ (on $A$) is well-founded iff it is a well-ordering (on $A$).

($\mathsf{Wellf}(<)$) $\quad \forall Q.\ \big(\ \exists x.\ Q(x) \quad\Rightarrow\quad \exists m.\ (\ Q(m) \wedge \neg\exists w{<}m.\ Q(w)\ )\ \big)$

($\mathsf{N}$) $\quad \forall P.\ \left(\ \forall x.\ P(x) \quad\Leftarrow\quad \exists{<}.\ \left(\begin{array}{l} \forall v.\ (\ P(v) \ \Leftarrow\ \forall u{<}v.\ P(u)\ ) \\ \wedge\ \mathsf{Wellf}(<) \end{array}\right)\right)$

($\mathsf{S}$) $\quad \forall P.\ \big(\ \forall x.\ P(x) \quad\Leftarrow\quad P(\mathsf{0})\ \wedge\ \forall y.\ (\ P(\mathsf{s}(y)) \Leftarrow P(y)\ )\ \big)$

($\mathsf{nat1}$) $\quad \forall x.\ (\ x=\mathsf{0}\ \vee\ \exists y.\ x=\mathsf{s}(y)\ )$

($\mathsf{nat2}$) $\quad \forall x.\ \mathsf{s}(x)\neq\mathsf{0}$

($\mathsf{nat3}$) $\quad \forall x,y.\ (\ \mathsf{s}(x)=\mathsf{s}(y)\ \Rightarrow\ x=y\ )$

It is important to note that ($\mathsf{N}$) is a *theorem* and not an axiom. This means that there is no reason at all to explain the justification for applying ($\mathsf{N}$). This is different for the case of an axiom, such as the Axiom of Structural Induction ($\mathsf{S}$). There is no need to discuss potential use of the actual infinite in this context. Assuming two-valued (i.e., classical) logic, there is also no need to discuss apagogic vs. positive reasoning, or whether a *reductio ad absurdum* may be useful in a proof.

I suggest that we restrict our discussion to two-valued logic because the topic is already sufficiently complicated without other logics, such as intuitionistic logic; cf. Heyting (1930). Moreover, for the relevant time until 1900, all logics in mathematics are two-valued.

For two-valued logic, the theorem $(\mathsf{N})$ is indeed a trivial one, simply because $\mathsf{Wellf}(<)$ is equivalent to its contrapositive, which is equivalent to $\mathsf{Wellf}(<)'$.

$$(\mathsf{Wellf}(<)') \quad \forall P.\ \Big(\ \forall x.\ P(x) \quad \Leftarrow \quad \forall m.\ \big(\ P(m) \ \Leftarrow\ \forall w{<}m.\ P(w)\ \big)\ \Big)$$

The natural numbers are specified up to isomorphism by the axioms $(\mathsf{nat1})$ and $\mathsf{Wellf}(\mathsf{s})$, for the successor function $\mathsf{s}$ given by $\mathsf{s}(x) := x{+}1$.

$$(\mathsf{Wellf}(\mathsf{s})) \quad \forall Q.\ \Big(\ \exists x.\ Q(x) \quad \Rightarrow \quad \exists m.\ \big(\ Q(m) \wedge \neg\exists w.\ (\mathsf{s}(w){=}m \wedge Q(w))\ \big)\ \Big)$$

$$(\mathsf{Wellf}(\mathsf{s})') \quad \forall P.\ \Big(\ \forall x.\ P(x) \quad \Leftarrow \quad \forall m.\ \big(\ P(m) \ \Leftarrow\ \forall w.\ (\mathsf{s}(w){=}m \Rightarrow P(w))\ \big)\ \Big)$$

Using $(\mathsf{nat1})$, $(\mathsf{nat2})$, and $(\mathsf{nat3})$ this can be simplified to the following logically equivalent formulas, which are variants of the Axiom of Structural Induction $(\mathsf{S})$.

$$(\mathsf{Wellf}(\mathsf{s}))' \quad \forall Q.\ \Big(\ \exists x.\ Q(x) \quad \Rightarrow \quad \big(\ Q(0) \vee \exists y.\ \big(\ Q(\mathsf{s}(y)) \wedge \neg Q(y)\ \big)\ \big)\ \Big)$$

$$(\mathsf{Wellf}(\mathsf{s})')' \quad \forall P.\ \Big(\ \forall x.\ P(x) \quad \Leftarrow \quad \big(\ P(0) \wedge \forall y.\ \big(\ P(\mathsf{s}(y)) \Leftarrow P(y)\ \big)\ \big)\ \Big)$$

Note that $\mathsf{Wellf}(<)$ and $(\mathsf{nat1})$ are similar to the axioms of Mario Pieri (1860–1913) (cf. Pieri (1907)), with the exception that Pieri avoids a name for the $\mathsf{0}$.[1]

According to Lemma 2.1 of (Wirth, 2004), $\mathsf{Wellf}(\mathsf{s})$ implies $\mathsf{Wellf}(\prec)$ for the ordering of the natural numbers $\prec$, i.e., the transitive closure of $\mathsf{s}$. Thus, the natural numbers are born with the following instance of Nötherian induction on $\prec$.

$$(\mathsf{N}') \quad \forall P.\ \Big(\ \forall x.\ P(x) \quad \Leftarrow \quad \big(\quad \forall v.\ \big(\ P(v) \quad \Leftarrow \quad \forall u{\prec}v.\ P(u)\ \big)\ \big)\ \Big)$$

Regarding logic and the justification and soundness of proofs, everything should be clear now.

## 2 Methods

So let us come to proof methods. The most simple lingual representation is Fermat's *descente infinie*: For an assumed arbitrary counterexample, show the existence of another counterexample which is smaller in $\prec$!

This is all what a working mathematician has to do. What he thinks when he does this is irrelevant from a mathematical point of view. On the one hand, he might think about an actual infinity of smaller counterexamples (indefinite descent), and see the proof as a *reductio ad absurdum*. On the other hand, he might think about some small values for which the theorem is true and into which the reductive process starting from an assumed counterexample would have to crash, and see the proof as a form of apagogic reasoning. In any case, the reasoning is merely hypothetical. The infinite is not involved.

Compared to all other forms of induction, *descente infinie* is more useful or at least just as useful under practical methodological aspects.

[1] I was not able to understand the sentence "In order to infer the principle of complete induction from Pieri's axioms, it is necessary not only that a minimum exists, but also that such a minimum is unique." [Bussotti (2006), p.466f.] I was not able to read (Di Leonardo and Marino, 2001), simply because I am too stupid to read any languages besides German, English, Latin, French, and Dutch.

Moreover, *descente infinie* typically offers some advantages for representation of proofs in natural language.

Finally, *descente infinie* may be also superior under the aspect of non-two-valued logics, but I am not interested in this topic here.

# 3 Foundations of Mathematics

From a foundational point of view, one should note that the infinitely descending sequences may not exist, even if we take an ordering that is not well-founded. I will discuss this here for the case of the natural numbers because it might have to do with the philosophical differences between indefinite descent and reduction-descent.

Well, if anything needs discussion, then it is the second-order axiom $\mathsf{Wellf}(\mathsf{s})$, which is equivalent to the second-order Axiom of Structural Induction ($\mathsf{S}$).

We could say that every natural number has the form $\mathsf{s}^n(\mathsf{0})$ for a natural number $n$. Then it is clear that we have to get to $\mathsf{0}$ after $n$ steps of taking the predecessor. This explanation, however, is of little epistemological value because it just applies the natural number $n$ from the meta level for the explanation the natural numbers of the object level.

If we suppose a non-well-founded successor relation $\mathsf{s}$, surprisingly this does not mean that we also have an infinitely descending $\mathsf{s}$-chain, simply because we cannot name this chain in any (formal) language. If we have the Axiom of Choice to our disposal, then the infinitely descending $\mathsf{s}$-chain must exist. Otherwise not.

So if you insist on the descending chains (for which there is no reason in mathematics, but maybe in philosophy or history), then I can see the following difference w.r.t. the foundations of mathematics between indefinite descent and reduction-descent. The origin of this view of mine is based more on the München privatissimum than on (Bussotti, 2006).

For the existence of the infinitely descending chain required for indefinite descent you need a weak form of the Axiom of Choice, namely the Principle of Dependent Choice, cf. § 2.1.2 of (Wirth, 2004).

For the existence of the arbitrarily long finite chain required for reduction-descent you do not need (any weak forms of) the Axiom of Choice, provided that you can explicitly describe the smaller counterexample in terms of the given one.

But then your classification lacks an important intermediate notion. Suppose that you can show that the smaller counterexample cannot be named explicitly, but that it is possible to show that there is a *finite* set of smaller counterexamples for any given one. This is typically the case because a proof, say the only one explicitly given by Fermat as discussed in (Wirth, 2006), exhibits a finite set of smaller counterexamples in a finite number of cases. Then you need only König's Lemma to construct the infinitely descending $<$-chain. König's Lemma is a *strictly* weaker form of the Axiom of Choice than the Principle of Dependent Choice, i.e. if there are models of set theory where König's Lemma holds, then there are models of set theory where König's Lemma holds but the Principle of Dependent Choice does not hold.

# 4 My München View

Let us assume that you are right that we have to differentiate between indefinite descent and reduction-descent, say for historiographical purposes.

The reduction-descent is a proper sub-method of the method of indefinite descent. This means that, in any case, if the applicability conditions of the method of reduction-descent are satisfied, then

1. the applicability conditions of the method of indefinite descent are satisfied, and
2. the sequence of proof steps of a proof by reduction-descent satisfies the requirements of a proof by indefinite descent.

Indeed:

ad 1. The method of reduction-descent is applicable to all irreflexive orderings $<$ for which the set $\{\ a \mid a{<}b\ \}$ has a finite cardinality for any $b$. By finitistic inspection of this set we immediately can conclude that such an ordering is a well-founded relation. Thus, the method of indefinite descent is applicable.

ad 2. If we name one unique smaller counterexample, then there exists a smaller counterexample.

Abstracting from the concrete situation of the natural numbers, talking in terms of an irreflexive ordering $<$, we thus get:

| | applicability condition | agenda |
|---|---|---|
| Reduction-descent | $\{\ a \mid a{<}b\ \}$ is finite for any $b$. | Give an algorithm to compute from an arbitrary counterexample another counterexample that is smaller in $<$ w.r.t. a recursive weight function. |
| Indefinite descent | $<$ is well-founded. Or does this have the same restriction as reduction-descent here? | For an arbitrary counterexample, show the existence of another counterexample that is smaller in $<$ w.r.t. a weight function. Do we need an algorithm (i.e., computability) here? Do we need recursiveness of the weight function? |
| Descente infinie | $<$ is well-founded | For an arbitrary counterexample, show the existence of another counterexample that is smaller in $<$ w.r.t. a weight function. Recursiveness and constructiveness are nowhere required in this process. The cardinality of the smaller counterexamples used in the argumentation is not required to be finite. |

According to his letter for Huygens (cf. Fermat (1891ff.), Vol.1, p.431f.) I think that the name *descente infinie* is justified for the above method. The only difference of the method that I call *descente infinie* to Fermat's description is that he speaks of a sequence descending to infinity instead of a non-well-founded set. But this difference, manifesting itself in the Principle of Dependent Choice, was clearly not perceivable before 1900.

# 5 The Question

**Do you agree with all of my points?**

**Are there still some minor differences in our views?**
**Which ones?**

**Please also do answer my open question in the above table!**

Sincerely,
CP

# References


Berka, K., Kreiser, L. (Eds.), 1973. Logik-Texte – Kommentierte Auswahl zur Geschichte der modernen Logik. Akademie-Verlag, Berlin, 2nd rev. ed. (1st ed. 1971; 4th rev. rev. ed. 1986).

Bussotti, P., 2006. From Fermat to Gauß: indefinite descent and methods of reduction in number theory. No. 55 in Algorismus. Dr. Erwin Rauner Verlag, Augsburg.

Di Leonardo, M. V., Marino, T., 2001. Il principio del minimo interio è equivalente al principio di induzione completa? Quaderni della riceria in didattica 10.
URL `http://math.unipa.it/~grim/pieri3.pdf`

Fermat, P., 1891ff.. Œuvres de Fermat. Gauthier-Villars, Paris, Ed. by Paul Tannery, Charles Henry.
URL `http://fr.wikisource.org/wiki/%C5%92uvres_de_Fermat`

Heyting, A., 1930. Die formalen Regeln der intuitionistischen Logik. Sitzungsberichte der Preußischen Akademie der Wissenschaften, Berlin, Physikalisch-mathematische Klasse II 1930, 42–56, short version also in: Berka and Kreiser (1973), pp. 173–178.

Pieri, M., 1907. Sopra gli assiomi aritmetici. Il Bollettino dell'Accademia Gioenia di Scienze Naturali, Catania ?, 26–30.

Wirth, C.-P., 2004. *Descente Infinie* + Deduction. Logic J. of the IGPL 12, 1–96.
URL `http://www.ags.uni-sb.de/~cp/p/d`

Wirth, C.-P., 2006. A Self-Contained and Easily Accessible Discussion of the Method of Descente Infinie and Fermat's Only Explicitly Known Proof by *Descente Infinie*. SEKI-Working-Paper SWP–2006–02 (ISSN 1860–5931). SEKI Publications, Saarland Univ.
URL `http://www.ags.uni-sb.de/~cp/p/fermatsproof`