EasyChair Preprint

№ 3357

Fermat's Last Theorem Proved by Induction

Vasil Penchev

May 10, 2020

FERMAT'S LAST THEOREM PROVED BY INDUCTION

Vasil Penchev, vasildinev@gmail.com
Bulgarian Academy of Sciences: Institute of Philosophy and Sociology:
Dept. of Logical Systems and Models

Abstract. *A proof of Fermat's last theorem is demonstrated. It is very brief, simple, elementary, and absolutely arithmetical. The necessary premises for the proof are only: the property of identity of the relation of equality,* modus tollens*, axiom of induction, the proof of Fermat's last theorem in the case of "*n = 3*" as well as the premises necessary for the formulation of the theorem itself. It involves a modification of Fermat's approach of infinite descent. The infinite descent is linked to induction starting from "*n = 3*" by* modus tollens*. An inductive series of* modus tollens *is constructed. The proof of the series by induction is equivalent to Fermat's last theorem. As far as Fermat had been proved the theorem for "n = 4", one can suggest that the proof at least for "n ≥ 4" had been accessible to him.*

The theorem known as "Fermat's last theorem" (FLT) was formulated by the French mathematician in 1637 and proved by Andrew Wiles (1995). Fermat remained both its statement and his claim for the proof too long for the margin. So, the challenge of a simple proof accessible to Fermat has been alive for centuries.

Andrew Wiles's proof is too complicated. It is not only beyond arithmetic, but even the question whether it is within set theory can be asked (whatever the answer might be).

What follows is a simple and elementary proof by the axiom of induction applied to an enumerated series of uniform recurrent arithmetical statements sharing the logical form of *modus tollens*.

The necessary premises are only: the identity of equality in mathematics; *modus tollens*; the axiom of induction, the proof of FLT for $n = 3$. All premises necessary for the theorem itself to be formulated should be added as well as propositional logic for the proof itself. Thus, all Peano axioms of arithmetic and those of propositional logic are included.

The set of all natural numbers, designated as "N", is the only set meant anywhere bellow. All variables (x, y, z, n, a, b) and the constant "c" are defined only on it: their values are its elements. However, the set "N" (as an actual infinite set in the sense of set theory) is not used. It is utilized only for simplifying the notations.

The idea of proof is a modification of Fermat's infinite descent, consisting in the following: The modification is not directed to construct a false statement included in any proof by *reductio ad absurdum*. Furthermore, it starts as if "from infinity" rather than from any finite natural number. Anyway, the modification is able to be restricted only to arithmetic and the axiom of induction (i.e. without the set-theory "actual infinity") by means of an enumerated series of *modus tollens*. Thus, Fermat's infinite descent is seen and utilized as "reversed": as an ascent by induction.

If one decomposes FLT to an enumerated series of statements, namely, FLT (3), FLT (4), FLT (5), …, FLT (n), FLT (n+1) , ..., each of one referring to a certain natural number, 3, 4, 5, n, n=1, … , which is the exponent in FLT, the idea of the proof is:

$$\forall(x,y,z,n)\,\epsilon\,N\colon[(a=x^{n+1})\rightarrow(b=x^{n})]\leftrightarrow\ [FLT(n)\ \rightarrow\ FLT(n+1)]$$

According to FLT, all FLT (n) are negative statements. If one considers the corresponding positive statements, FLT*(n) = ¬FLT (n), the link to the series of *modus tollens* is obvious:

$$\forall(x,y,z,n)\epsilon\,N\colon[(a=x^{n+1})\rightarrow(b=x^{n})\leftrightarrow[\neg\text{FLT*(n)}\rightarrow\neg\ \text{FLT*(n+1)}]$$

This is the core of proof. It needs a reflection even philosophical.

Two triple equalities ("$a=x^{n+1}=y^{n+1}+z^{n+1}$", and "$b=x^{n}=y^{n}+z^{n}$") are linked to each other by *modus tollens*. What is valid for the left parts, $(a=x^{n+1})\rightarrow(b=x^{n})$, is transferred to the right parts, $\neg(x^{n}=y^{n}+z^{n})\ \rightarrow\neg(x^{n+1}=y^{n+1}+z^{n+1})$, as an equivalence. The mediation of each middle member in both triple equalities is crucial: it allows for the transition. An extended description of "$\forall(x,y,z,n)\epsilon\,N\colon[(a=x^{n+1})\rightarrow(b=x^{n})\leftrightarrow\ [\neg$FLT*(n) $\rightarrow\neg$ FLT*(n+1)]" is:

$$\forall(x,y,z,n)\epsilon\,N\colon[(a=x^{n+1}=y^{n+1}+z^{n+1})\rightarrow(b=x^{n}=y^{n}+z^{n})]\leftrightarrow$$
$$\leftrightarrow[\neg(b=x^{n}=y^{n}+z^{n})\rightarrow\neg(a=x^{n+1}=y^{n+1}+z^{n+1})]$$

In fact, the arithmetical equality ("=") and logical equality "↔" are divided disjunctively. Their equivalence is not necessary or used.

Anyway, their equivalence is valid as a mathematical isomorphism. Even more, the law of identity in logic, "$\forall a\colon a\leftrightarrow a$", referring to the propositional logic, and the axiom of identity, "$\forall a\colon a=a$", referring to any set of objects in a (first-order, second-order, ..., n-order, ...) logic are isomorphic mathematically. The identity is a special kind of relation, in which all those orders are merged, and thus, indistinguishable from each other within it.

Nonetheless, any exemplification of that indistinguishability of identity due to mathematical isomorphism is not used in the proof. Furthermore, the auxiliary variables "*a*" and "*b*" (involved only for the explanation of the idea) will not be utilized.

The proof in detail:

$$\text{FLT}\colon\forall(x,y,z,n\geq3)\,\epsilon\,N\colon\neg\text{"}x^{n}=y^{n}+z^{n}\text{"}$$

"FLT(c)" means: ¬"$x^{c}=y^{c}+z^{c}$" where "c" is a constant: $c\geq3,\ c\,\epsilon\,N$. FLT will be proved as FLT(c) will be proved for each "c" ($\forall c$) by induction. The equivalence of "FLT" and "∀c: FLT(c)" is granted as obvious. The set of all "FLT(c)" is neither used nor involved in any way.

The relation of equality can be defined by its three properties: identity, symmetry, and transitivity. Only "identity" will be used to be proved a corollary from *modus tollens*, which is necessary to be linked Fermat's infinite descent to an inductive ascent.

Law (axiom) of identity [LI]: $\forall A\colon A = A$

For the present utilization, it will be modified equivalently to:

(A) "$\forall x\colon x \leftrightarrow x = x$", and then to

(B) "$(\forall x\colon x = y) \leftrightarrow (\forall x\colon x \leftrightarrow x = y)$".

Proof:

A: (1) $x \to (x = x)$. Indeed, let $\neg\,(x \to x = x) \to \exists x\colon x \neq x \to \neg\,(\forall x\colon x = x)$: contradiction.

(2) $(x = x) \to x$. Indeed: if not, the term "x" of the proposition "$x = x$" would be absent sometimes: contradiction.

B: $\forall x\colon x \leftrightarrow (x{=}x) \leftrightarrow [x = (x = y)] \leftrightarrow (x = x = y) \leftrightarrow [(x = x) = y] \leftrightarrow (\mathrm{x} = \mathrm{y})$.

Consequently, $\forall x\colon x \leftrightarrow (x{=}y)$

"A" $\wedge$ "B" $\to$ "$(x = x) \leftrightarrow (x = y)$" which is necessary for *modus tollens* to be equivalently modified.

Modus tollens [MT]: $(A \to B) \leftrightarrow (\neg B \to \neg A)$, and it modified for the case [MMT]:

$$[("x^{n+1} = x^{n+1}" \to "x^n = x^n") \leftrightarrow (\neg "x^n = x^n" \to \neg "x^{n+1} = x^{n+1}")] \leftrightarrow$$
$$\leftrightarrow [("\boldsymbol{x^{n+1} = x^{n+1}}" \to "\boldsymbol{x^n = x^n}") \leftrightarrow (\neg "\boldsymbol{x^n = y^n + z^n}" \to \neg "\boldsymbol{x^{n+1} = y^{n+1} + z^{n+1}}")]$$

Axiom of induction [AI]: $"\forall p, n\colon p(1) \wedge [p(n) \to p(n+1)] \to p"$ where "$p(n)$" is an arithmetical proposition referring to the natural number "n", and "p" is the same proposition referring to all natural numbers. "Arithmetical proposition" means a proposition in a first-order logic applied to arithmetic. The axiom of induction is modified starting from $n = 3$ rather than from $n = 1$:

$$\{\forall p, n\colon p(1) \wedge [p(n) \to p(n+1)] \to p\} \to \{\forall p, n \geq 3\colon p(3) \wedge [p(n) \to p(n+1)] \to p\}$$

A modification of Fermat's infinite descent [MFID]: MT modified as above is applied as starting from $n = 3$ as follows:

$$\ldots n, n-1, \ldots 5, 4, 3$$

The same descent is interpreted as a series of enumerated propositions:

$$\ldots (n), (n-1), \ldots (5), (4), (3)$$

A reverse chain of negations is implied:

$$\neg(3), \neg(4), \neg(5), \ldots, \neg(n-1), \neg(n), \ldots$$

Both ascent of "negations" and infinite descent are constructed step by step following the increasing number of the negative propositions (rather than the decreasing number of the positive propositions):

$$[(4) \to (3)] \leftrightarrow [\neg(3) \to \neg(4)], [(5) \to (4)] \leftrightarrow$$
$$[\neg(4) \to \neg(5)], [(6) \to (5)] \leftrightarrow [\neg(5) \to \neg(6)], \quad \dots$$
$$\dots [(n+1) \to (n)] \leftrightarrow [\neg(n) \to \neg(n+1)], [(n+2) \to (n+1)] \leftrightarrow$$
$$\leftrightarrow [\neg(n+1) \to \neg(n+2)], \dots \dots$$

So, one builds a series of *modus tollens* starting from $n = 3$.

FLT (3): x, y, z *are natural numbers. There do no exist any* x, y, z:

$$x^3 + y^3 = z^3$$

Many mathematicians beginning with Euler claimed its proof. Ernst Kummer's proof (1847) will be cited here for its absolute rigor. It refers to all cases of "regular prime numbers" defined by Kummer, among which the case "$n = 3$" is.

Furthermore, the "n^{th}" member of the series of *modus tollens*, namely:

"[(n+1)→(n)]↔[¬(n)→¬(n+1)]" is valid as far as "(n+1)→(n)" is valid.

@One interprets that "(n+1)→(n)" in the case of FLT:

$$\forall x, n: (x^{n+1} = x^{n+1}) \to (x^n = x^n)$$

This is true for "$x^{n+1} = x^{n+1} = x^n . x^1$". Thus, "$x^n = x^n$" is a necessary condition for "$x^{n+1} = x^{n+1}$" and the former is implied by the latter.

One uses [MMT] "modified *modus tollens*" further:

The series of modified *modus tollens* is interpreted in terms of FLT as the following series of implications:

$$[\text{“}x^4 \to x^3\text{”} \wedge \text{“FLT (3)”}] \to \text{“FLT (4)”}$$
$$[\text{“}x^5 \to x^4\text{”} \wedge \text{“FLT (4)”}] \to \text{“FLT (5)”}$$
$$[\text{“}x^6 \to x^5\text{”} \wedge \text{“FLT (5)”}] \to \text{“FLT (6)”}$$
$$\dots \to \dots$$
$$[\text{“}x^{n+1} \to x^n\text{”} \wedge \text{“FLT (n)”}] \to \text{“FLT (n+1)”}$$
$$[\text{“}x^{n+2} \to x^{n+1}\text{”} \wedge \text{“FLT (n+1)”}] \to \text{“FLT (n+2)”}$$
$$\dots \to \dots$$

The member of the series of implications is true for "n=3", the validity for "n" implies the validity for "n+1". Thus, it is valid for "any member enumerated by a natural number greater than two" in virtue of the axiom of induction.

FLT is proved.

If one accepts that Fermat (1670) had proved FLT (4) and as far as the above proof seems to be accessible to him, he might prove FLT at least for $n \geq 4$.

The answer of a frequent objection:

The objection is: the "modified *modus tollens*" needs "$x^n = y^n + z^n$" to be proved. Fermat's infinite descent modified as in the claimed proof uses the substitution "$\neg(x^n = y^n + z^n)$". So, this contradiction, involved in the proof, makes it false.

The answer is: "$x^n = y^n + z^n$" is a necessary condition for the "modified *modus tollens*". Thus, the latter implies the former. "$\neg(x^n = y^n + z^n)$" is a substitution in the "modified *modus tollens*". Thus, the latter implies the former.

Consequently, the "modified *modus tollens*" implies both "$x^n = y^n + z^n$" and "$\neg(x^n = y^n + z^n)$", but **separately**, i.e. by disjunction rather than by conjunction. This is not a contradiction as:

$$[(a \to b) \vee (a \to \neg b)] \leftrightarrow "True"$$
$$\forall x: ("True" \to x) \leftrightarrow x$$

This means only that the proof involves a tautology redundant to the syllogism.

This is quite different from the alleged "$[a \to (b \wedge \neg b)] \to "False$", which is absent in the proof.

References:

Fermat, P. (1670) "Diophanti Alexandrini Arithmeticorum libri sex, et De numeris multangulis liber unus. Cum commentariis C.G. Bacheti v.c. & obseruationibus D.P. de Fermat .senatoris Tolosani," in *Acessit Doctrinae analyticae inuentum nouum, collectum ex varijs eiusdem D. de Fermat epistolis.* Tolosae: Excudebat Bernardus Bosc, è regione Collegii Societatis lesu, M. DC. LXX, pp. 338-339 (Source: http://books.google.com/books?id=yx9VIgeaCEYC&hl=&source=gbs_api 1670.)

Wiles, A. (1995) "Modular Elliptic Curves and Fermat's Last Theorem," *Annals of Mathematics* Second Series **141** (3): 443-551 (DOI 10.2307/2118550. MR1333035. Zbl 0823.11029)

Kummer, E. (1847) "Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ," in Kummer, Ernst Eduard. *Collected papers* (ed. Andre Weil) Volume 1. *Contributions to number theory*. Berlin, Heidelberg, New York: Springer, 1975, pp. 274-297. (ISBN 978-3662-48832-4. DOI N/A. MR0465760. Zbl 1331.01037.)